Public Safety and Emergency Preparedness Canada
Critical Infrastructure Protection and Emergency Preparedness

Sécurité publique et Protection civile Canada
Protection des infrastructures essentielles et Protection civile

CHARACTERIZATION AND RANKING OF LINKS CONNECTING LIFE SUPPORT NETWORKS

104-06736/

Acknowledgments

This publication has been prepared for:

Public Safety and Emergency Preparedness Canada

2nd Floor, Jackson Bldg.
122 Bank St.
Ottawa, ON K1A 0W6
Tel: (613) 944-4875
Toll Free: 1-800-830-3118
Fax: (613) 998-9589
Email: communications@ocipep-bpiepc.gc.ca
Internet: www.ocipep-bpiepc.gc.ca

Authors:

Benoît Robert, P.Eng., Ph.D.
Marie-Hélène Senay
Marie-Ève P. Plamondon
Jean-Pierre Sabourin

Risk and Performance Centre
École Polytechnique de Montréal

This material is based upon work supported by the Division of Research and Development (DRD) in the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), under Contract Reference No. 2002D001. OCIPEP is now a part of Public Safety and Emergency Preparedness Canada (PSEPC). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Public Safety and Emergency Preparedness Canada.

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA (2003)
Catalogue No.: D82-88/2003E-PDF
ISBN: 0-662-35684-5

Executive Summary

Certain infrastructures and networks of infrastructures, called Life Support Networks (LSNs) or Critical Infrastructures (CI), allow our society's socio-economic activities to be carried out and supported. Because of their missions, these infrastructures must be kept operational both on a daily basis and in times of crisis. The catastrophic events experienced in recent years (e.g., the 1998 Ice Storm in Quebec and Ontario and floods in the Saguenay) emphasized our dependence on these networks and highlighted the importance of constantly improving emergency measures.

One approach to improved emergency management is to identify the most critical infrastructures and give them priority when planning emergency and mitigation measures. This requires an understanding of the complexity of these infrastructures and in particular their interdependencies. While recognized as important, infrastructure interdependencies are poorly understood and rarely accounted for in emergency measures planning. This report studies the issue of prioritizing links between LSNs for purposes of mitigation and emergency measures planning. The aim was to develop a ranking methodology, based on a criticality scale, using a pragmatic, non-subjective and consistent method for all the disciplines involved.

A brief review of existing documentation on the notion of infrastructure criticality indicated that current techniques focus on infrastructures as a whole, rather than on links between infrastructures, and are generally not based on a systematic underlying methodology. Further, there is minimal ongoing research that deals specifically with links between LSNs. A preliminary framework for classifying and ranking LSNs is therefore presented as a stepping-stone to a more detailed discussion on links. In this context, links between LSNs are defined and their characteristics explored. Criticality level evaluation criteria are developed based on three practical concepts from emergency management, namely vulnerability, the impact of failures, and the operational potential for managing emergency measures. These components are then used to construct and demonstrate a novel ranking methodology for links between LSNs.

There is clear potential for methodologies focused on studying links between LSNs to assist in reducing vulnerability and risk. Further work is required in order to develop operational, robust methodologies for emergency managers. It is noted that any ranking of links between infrastructures will depend on the operational goals and priorities of the emergency manager. Therefore, criticality itself must be considered variable rather than a fixed absolute. Lastly, the impact and nature of cyberlinks are not well understood and require further study.

Table of Contents

Acknowledgments ii

Executive Summary iii

1.0 Project Background 1

2.0 Criticality: Status 2

2.1 Canadian Approach 2
2.2 American Approach 3
2.2.1 Sample Ranking Scheme: The Homeland Security Advisory System 4
2.3.1 Situation Assessment 4
2.3.2 Risk Identification Criteria 5
2.4 Analysis and Recommendations 5

3.0 Definition and Classification of Life Support Networks 7

3.1 Definition and Characteristics of Life Support Networks 7
3.2 Classification of Life Support Networks 9

4.0 Links Among Life Support Systems 12

4.1 Definition of Links 12
4.1.1 Direct Links 12
4.1.2 Indirect Links 13
4.1.3 Cyberlinks 13
4.2 Link Categorization 14
4.3 Link Ranking 15
4.4 Characterization Criteria 16
4.4.1 Link Vulnerability 17
4.4.2 Impacts of Link Failure 18
4.4.3 Emergency Measures Management Operational Potential of Links 19
4.5 Identification Parameters and Evaluation Scale 20

5.0 Ranking Methodology 24

5.1 Criticality Classes 24
5.2 Characterization Criteria 25
5.3 Methodology 25

6.0 Application 28

6.1 Calculation Example 28
6.2 Interpretation of Results 30
6.2.1 Ranking Possibilities 30
6.2.2 Variations in Criticality Levels 34
6.3 Method Uses 35

7.0 Conclusion 37

8.0 Bibliography 39

Appendix A – Link Characterization Grid **A-1**
Appendix B – Link Parameterization **B-1**
Appendix C – Validation **C-1**

1.0 Project Background

Work undertaken prior to this project relating to domino effects among Life Support Networks (LSNs) is part of a national and international trend towards establishing effective and efficient management plans for these networks based on the contradictory notions of maximum production and minimum risk (Robert, 2002b; SEVESO, 2000). This management must be based on a detailed knowledge of the networks and of the interactions among them in order to be able to assess the various impacts of failures. At present, most risk studies attempt to evaluate the risk based on a single economic, technical or industrial result (Stedinger, 1996). Moreover, these studies only deal with a small number of specific events that might lead to a failure (Can/Csa, 1991). These failures have far-reaching impacts, not only on people but also on socio-economic activities. Some of these impacts, such as the physical effects of a flood, are tangible, concrete and easy to identify. Others, however, are much more subtle and require an exhaustive analysis to determine all the impacts caused by the partial or complete failure of a network: an oil pipeline leak contaminates soil, arable land, waterways, the drinking water system, and so on. In such cases, it is difficult to evaluate all the impacts.

Earlier work on interactions among LSNs has shown that networks are highly interdependent. These interdependencies stem from the existence of multiple links between the networks. These links allow, among other uses, the transfer of substances and services from one network to another. Although these links are necessary for network operation, they increase the risk of failures by allowing the transfer of the vulnerabilities of one network to another. It seems that a comprehensive methodology for studying vulnerability and risk based on defining, characterizing and evaluating these links might make it possible to reduce domino effects among life support networks (Robert, 2001 and 2002a). A link allows vulnerabilities to impact other networks through repercussion. The methodology will thus attempt to define the vulnerability of the original component, the repercussion function characterized by repercussion curves and, finally, the destination vulnerability.

2.0 Criticality: Status

A brief literature review on the notion of criticality was undertaken to find out what the status of the issue is and to determine whether current developments can be used in our work on links among networks. The information available at the time of this project deals primarily with critical infrastructures in a broad sense rather than on links between networks. It does, however, make it possible to establish a strong relationship with work on life support networks since these facilities are considered by many organizations and authors as being necessary for proper socio-economic functioning and the welfare of citizens. At present, work is being carried out throughout the world to determine which infrastructures can be identified as being critical. The approaches recommended in Canada and the United States will be presented, followed by a discussion based on the potential uses of these results.

2.1 Canadian Approach

According to the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), Canada's critical infrastructure "consists of those physical and information technology facilities, networks and assets, which if disrupted or destroyed would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada" (Emergency Preparedness Digest, 2001; OCIPEP, 2001).

They are divided into six sectors:

- **Energy and public utilities**: electricity, gas and oil distribution
- **Key communications**: telecommunications, radio broadcasting, Internet, the telephone system, television and satellites
- **Transportation**: air, rail, water and land lines
- **Security**: nuclear safety, 911 services (police, fire, ambulance), search and rescue
- **Financial, food and health services**: banks, agriculture, food distribution, health care, water treatment, hospitals, pharmacies
- **Critical government services**: facilities, networks, major government assets, pension plans, employment insurance, immigration, weather forecasting, education, social benefits

Following this preliminary classification, which represents the major activity sectors, it seems important to understand the criteria used to make it and to determine whether it can be used to determine what infrastructures are more critical than others. However, like classifying critical infrastructures in different sectors, there is no information indicating that there is any systematic process for recognizing whether some infrastructures are more important than others. This Canadian government classification does, however, allow us to identify critical operating points in society. However, a precise classification opening up the possibility of ranking these infrastructures would allow processing priorities to be defined based on infrastructure criticality.

2.2 American Approach

The American definition of critical infrastructures is similar: critical infrastructures are those "systems and assets, whether physical or virtual so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national health or safety, or any combination of those matters" (*U.S.A Patriot Act*). The *National Strategy for the Physical Protection of Critical and Key Assets* published in 2003 by the Department of Homeland Security defines critical infrastructure sectors as follows:

- Agriculture and Food
- Water
- Public Health
- Emergency Services
- Defence Industrial Base
- Telecommunications
- Energy
- Transportation
- Banking and Finance
- Chemicals and Hazardous Materials
- Postal and Shipping

Following the attacks on the World Trade Center, the U.S. administration also deemed it necessary to define key assets to protect. These are:

- national monuments and icons
- nuclear power plants
- dams
- government facilities
- commercial key assets

The American definition of sectors and critical infrastructure systems does not include parameters or criteria that would allow this classification to be generalized. In its method, the North American Electric Reliability Council (NERC, 2002a and 2002b) opted to analyze electric power system risk and vulnerability. Thus, this major energy organization's strategy is to first identify critical infrastructures, the vulnerabilities inherent to each and finally, mitigation measures to be taken. Infrastructures are classified and ranked in terms of potential vulnerabilities. Criticality is thus defined here according to the vulnerability of electricity production, transportation and distribution facilities.

A preliminary classification of critical infrastructures has already been put forth by government agencies that have been charged with defining the criticality of these infrastructures. They are normally classified by sector, without any constant criteria for determining why they are critical. This lack of criteria for justifying the classification and prioritizing critical infrastructures explains the variety of definitions of criticality and structures identified as being critical. This lack of consistency in criteria for determining what infrastructures are critical thus clearly opens the way to interpretation of the definition of the concept of criticality. It seems that the

classification and ranking of these infrastructures needs to be supported by precise and tangible criteria that incorporate the notion of links among these facilities and provide some consistency in the data used and in the interpretation of this data.

2.2.1 Sample Ranking Scheme: The Homeland Security Advisory System

The events of September 11, 2001 confirmed the international trend of implementing increased emergency, mitigation and civil protection measures due to the increased number of natural disasters experienced in recent years. As part of a major reorganization of their national defence strategy, the United States created the Department of Homeland Security (DHS). This organization is in charge of the Homeland Security Advisory System (HSAS) which was set up by the Bush administration in March 2002 (White House, 2002). This reform was aimed not only at countering terrorist threats on American soil but also at developing a common vocabulary, structure and framework for discussion among the various stakeholders. The DHS's mission is to identify potential terrorist threats in the country and to communicate this threat with the help of the HSAS. It also has the task of drawing up a list of specific actions to take in order to protect the country and its citizens, institutions and facilities. Although this index is not intended to characterize critical infrastructures or links, it does provide a concrete example of a ranking.

2.3.1 Situation Assessment

The level of risk indicated by the HSAS incorporates the probability of threats occurring and the seriousness of their impacts. A scale describes the status of the situation with five intervals indicating the threat level, each one associated with a colour:

- **Low** – the threat of a terrorist attack is low. In addition to appropriate protection measures, federal departments and agencies must apply certain specific security guidelines. Colour associated with this level: green.

- **Guarded** – the threat of a terrorist attack is nominal but does exist. Therefore, more extensive measures must be applied. Colour associated with this level: blue.

- **Significant** – the threat of a terrorist attack is significant. Protection measures are generalized to the various sectors of society. Colour associated with this level: yellow.

- **High** – the threat of terrorist attack is high and special measures apply. Colour associated with this level: orange.

- **Severe** – the threat of terrorist attack is severe and measures are extensive and numerous. Colour associated with this threat level: red.

This scale is accompanied by instructions consisting of practical advice and actions to be taken at the government, managerial and public levels in order to reduce the risk of threats occurring and their impacts if they do occur. Information is highly centralized – the threat condition is assessed by the Secretary of the DHS under the direct authority of the President of the United

States. Threat conditions can be assigned to the entire nation, a specific region, an industrial sector, etc. Likewise, they are reassessed regularly to determine what adjustments are needed.

2.3.2 Risk Identification Criteria

The criteria used to determine threat status are unknown or unavailable except for those listed below:

- At what level is the threat credible?
- At what level is the threat confirmed?
- At what level is the threat specific and/or imminent?
- How serious is the threat?

These criteria are used to associate various sources of threats with a more or less serious state of terrorist threat. They do not describe the situation, but rather are interpretative.

This strategy of centralizing American government decisions seems to be a means of involving society in emergency preparedness for the country and its institutions as well as protecting the public. However, these criteria can lend themselves to subjective interpretation since they use disparate and non-homogeneous data. This classification and ranking of threat conditions in fact are used to direct the efforts of civil society and thus to control the implementation of prevention, emergency and mitigation measures at all levels.

2.4 Analysis and Recommendations

The methods used to classify or characterize critical infrastructures used by government agencies do not seem to be based on a systematic use of clearly established criteria. It is impossible to know whether there are specific evaluation criteria; if there are, how were they used to identify critical infrastructures? The data used to weight evaluation criteria should be quantifiable and measurable so it can be interpreted in the form of a meaningful scale. It would then be possible to create a ranking using a pragmatic, consistent and understandable approach for all stakeholders.

Moreover, the definition of critical infrastructures provided by government agencies divides them into sectors but does not indicate their order of priority in time of crisis. Of course, they are all critical to the proper functioning of society and to maintaining life, but this concept is too general for a meaningful classification to be made. The question that a ranking methodology must be able to answer is: what infrastructures are critical to achieve predetermined goals? This same question can be applied to links between infrastructures. In developing such a procedure, we must be willing to accept that criticality can vary depending on the situation and goals of the moment. Consequently, infrastructure or link ranking cannot be done for the long term and must remain flexible. This can be shown by a simple example. Consider two life support networks: an electric power distribution network and a water distribution network. Which of these should be deemed the more critical? The answer to this question depends on the goal to be achieved. If the goal is fire protection, the water network might be given priority. However, if the goal is to maintain economic activity, the electric power network might be considered as being the more

critical. It is because criticality varies depending on the situation and operational goals that any ranking concerning LSNs requires a methodology based on specific criteria that are precise but whose order of priority can be changed.

The notion of clearly defined criteria is therefore necessary for the development of a ranking methodology for links between LSNs. In order to be able to act in concert and maintain operational continuity in times of crisis, there must be a certain degree of standardization in ranking. It is essential that interpretation and subjectivity be limited. The criteria used must therefore be based on factual data and meet certain requirements. They must be:

- tangible
- understandable
- measurable
- unitary in terms of expertise and analysis
- based on available information
- ponderable

As to these specific characteristics, a practical approach based on effective and simplified application is needed. The methodological approach that will be developed must be standardized but flexible in order to juxtapose established criteria and concrete operational goals. It will then be possible to develop priority measures to protect or re-establish links among LSNs depending on foreseeable or existing events. These criteria must be ponderable in order for meaningful and non-symbolic ranking to be done.

It must be possible to track this process and explain it so that all those involved in emergency measure and mitigation planning can better understand the priority process.

This process must improve the transfer of emergency measure-related information. It will then be possible to limit the propagation of risks and reduce material and human losses when catastrophic events occur.

3.0 Definition and Classification of Life Support Networks

Although the methodology being developed will be specific to links, an understanding of the broader scope of application is required. To classify and rank links among life support networks in a coherent manner, it is important to perform a similar analysis on these networks. This network classification is beyond the scope of this research project, but this first approach is proposed as a stepping-stone to subsequent work on links. The principles governing this classification are similar to those used for links. Thus, even though the results are preliminary, the presentation in this section is useful and the results will be incorporated into the link ranking criteria.

Any classification activity must necessarily start with the essential activity of clarifying and defining what is to be studied. Thus, a prior definition of life support networks is given.

Life support networks are made up of a set of closely connected components. The components that directly support a network's mission form a main network, but there are parallel networks such as remote control systems and computer networks. Together, they form an integrated network whose reliability depends on the performance of each and every component. If a single component fails, the impacts at the system level depend not only on the importance of the component but also on the importance of the components affected by this failure. Moreover, components of several networks might be linked, resulting in multiple impacts caused by domino effects (Allen, 1997; Plate, 1996; Moses, 1998; Lemperiere, 1999).

The notion of life support networks is vast and networks are grouped based on their missions such as energy and public utilities, security, and so on. The goal of the proposed process is to show that a systematic approach allows us to classify life support networks using specific criteria. This classification is the first step in ranking and prioritizing life support networks based on unitary criteria using concrete and tangible information and data.

The proposed process is preliminary and must be validated by the entire emergency preparedness community. First, a definition of the networks is presented in order to properly delimit the problem. Based on this definition, a non-exhaustive list of life support networks is presented. Then, classification criteria are proposed and adapted to the networks previously identified.

3.1 Definition and Characteristics of Life Support Networks

The term "life support network" involves two important notions that must be clearly explained in order that the nature and characteristics of these networks can be understood.

- **Network** – A network may be generally defined according to two principles:
    - a set of infrastructures and links that physically or virtually branch out and intertwine. *Examples: water distribution network, electric power network, railroad network, telephone network.*
    - a set of infrastructures spread over a given territory that are directly or indirectly related to one another and generally governed by similar guidelines. *Examples: hospital network, food network, highway network, airport network.*

- **Life support** – These networks fulfil missions that are essential to the proper functioning of a society, providing critical services having to do with health, public security and the proper functioning of the economy.

Thus, life support networks are therefore made up of a multitude of infrastructures that ensure the proper functioning of economic and industrial activities and provide services that are essential to the needs of citizens (Denis, 2002; Selcuk, 1999; O'Leary, 1997). Thus, when a life support network fails, the human and socio-economic impacts are very serious and cannot be ignored (Hubbert, 1999). At present, life support networks are generally categorized in order to distinguish them from other networks that are not associated as much with socio-economic networks (Isenberg, 1991; Lau, 1995). However, this differentiation does not take the specific characteristics of these networks into account as to their effects or impacts on society.

As to this definition, seventeen life support networks have been identified by the authors. This list is not exhaustive, but was drawn up in order to validate the proposed methodology on networks with very different characteristics. They are briefly described here.

1. **Electric power network**: all infrastructures and operations used to produce, transport and distribute electricity. Electric power can be produced from various sources (gas, water, nuclear energy, etc.).
2. **Telecommunication network**: all infrastructures and operations used to communicate by means of wires, satellites, radio waves, etc.
3. **Computer network**: all infrastructures and operations used to utilize and transfer digitally encoded data and knowledge. These networks thus include not only computers with mechanisms for communicating among themselves but also, and most importantly, the knowledge contained in databases, management programs, simulators, etc. Remote control systems are included in these networks.
4. **Public transportation network**: all infrastructures and operations used to transport passengers within an urban area by road or rail.
5. **Natural gas network**: all infrastructures and operations used to extract, store, transport and distribute natural gas.
6. **Liquid fuel network**: all infrastructures and operations used to extract, process, store, transport and distribute liquid fuels.
7. **Rail network**: all infrastructures and operations used to transport, store and distribute goods and people by rail and train. Many different kinds of materials are transported.
8. **Water transportation network**: all infrastructures and operations used to transport, store and distribute goods and people by boat on rivers, lakes and oceans. Many different kinds of materials are transported.
9. **Sewage network**: all infrastructures and operations used to collect transport and treat sewage.
10. **Water network**: all infrastructures and operations used to supply, treat and distribute water to the public.
11. **Food network**: all infrastructures and operations used to produce, store, transport and distribute the products needed to feed people.
12. **Health network**: all infrastructures and operations having to do with public health care (hospitals, clinics, ambulances, etc.).

13. **Highway network**: all infrastructures and operations used to transport goods and people by means of roads, freeways, interchanges, overpasses, etc. Many different kinds of materials are transported.
14. **Airport network**: all infrastructures and operations used to transport goods and people by means of airplanes. Many different kinds of materials are transported.
15. **Financial network**: all infrastructures and operations having to do with financial services. This network includes banks, stock exchanges, automatic tellers, etc.
16. **Public security network**: all infrastructures and operations used to ensure the safety and protection of property and persons (police, fire, etc.).
17. **Government network**: all infrastructures and operations having to do with public administration (federal, municipal, etc.).

It seems that there are many life support networks that differ by their nature, function, materials transported, and so on. Studies on the vulnerabilities and impacts on these networks with respect to risks of anthropic origin must therefore be varied and distinctive. However, it is possible to group these networks systematically using specific criteria in order to make it easier to study them and associated domino effects with respect to risks, failures, vulnerability and impacts.

3.2 Classification of Life Support Networks

When grouping networks, we must consider their definition, missions, structures and interrelationships, their interactions with other networks, and their direct and indirect impacts on people. Thus, the following criteria were established to characterize and classify networks. These are preliminary criteria intended to validate the proposed methodology.

- **Intermeshing** – Determines whether the network is made up of infrastructures that are intermeshed or spread out over a territory, as defined in the definition of networks.
- **Materials transported** – Determines whether the network's main mission is to transport (and hold) a substance (water, gas, oil, food, etc.) or provide a service.
- **Interaction among networks** – Determines whether there are interactions (links) with other life support networks. These interactions may be evaluated:
    - qualitatively (very many, many, few, variable number, etc.);
    - quantitatively (more than 1,000, fewer than 10, etc.);
    - comparatively (more links, national average, etc.).
- **Impact on people** – Determines whether failure of a network would directly or indirectly impact people's lives.

Based on these criteria, life support network class criteria must be established to group networks with similar characteristics. These groupings are essential for evaluating risks, then incorporating them into management and performance evaluation mechanisms for these networks. Overall, evaluating the risks associated with life support networks requires carrying out vulnerability studies on the infrastructures of these networks as well as on operating and management mechanisms, combined with studies on impacts on people, socio-economic activities and the environment. Thus, the notion of interrelationships affects the nature of vulnerability studies and a direct impact on people is a significant classification criterion.

As to the above considerations, five classes of life support networks have been identified. They are as follows:

- **Class A** – Networks with intermeshed infrastructures, essentially used to provide services with a large number of interactions with other networks. The networks included in this class are:
  - electric power network
  - telecommunications network
  - computer network
  - public transportation network
    (*Transportation of persons is considered to be a service. Interactions with other networks involve people who use public transportation to go to work in other networks.*)

- **Class B** – Networks with intermeshed infrastructures, used to transport materials with many interactions with other networks. Examples of networks included in this class are:
  - natural gas network
  - liquid fuel network
  - rail network
  - sewer network

- **Class C** – Networks with intermeshed infrastructures used to transport materials with few interactions with other networks. This class differs from those above in that failure of these networks impacts people directly. So far, the only network included in this class is:
  - water network

- **Class D** – Networks with shared infrastructures used to provide services with a variable number of interactions with other networks. Failure of these networks impact people directly. Networks included in this class are:
  - food network
  - hospital network

- **Class E** – Particular networks class. They have shared or intermeshed infrastructures; they are used to transport people (which is considered to be a service) and many varied materials; they have a variable number of interactions with other networks. Failure of these networks impact people indirectly. Networks included in this class are:
  - highway network
  - airport network
  - marine transportation network
  - financial network
    (financial networks are intermeshed or shared and interactions with other networks are real but variable)

- public security network
  (impacts on people are variable but can be assumed to be indirect)
- government network

Table 1 below summarizes the classification described above.

Table 1 Characterization of life support network classes

Criterion	Life support network classes				
	A	**B**	**C**	**D**	**E**
Intermeshing	intermeshed infrastructures	intermeshed infrastructures	intermeshed infrastructures	shared infrastructures	shared or intermeshed infrastructures
Material transported	service	material	material	service	service or material
Interaction among networks	very many	many	few	variable	variable
Impact on people	indirect	indirect	direct	direct	indirect
Classification of networks	• electric • telecommunications • computer • public transportation	• natural gas • liquid fuels • rail • sewage	• water	• food • hospital	• highway • airport • marine transportation • financial • public security • government

The use of precise criteria, based on tangible concepts that rest upon notions of vulnerabilities, impacts and domino effects allow us to group the many life support networks in five distinct classes. This systematic approach must be followed when evaluating the importance of each of these classes based on precise criteria. Likewise, ranking and prioritization of these classes can be envisaged. These activities are important to all emergency measures planning processes. The advantage of this approach is that the prioritization results can and should differ depending on the criteria chosen. It is thus an evolving process that can be adapted to many different uses.

Within the specific framework of this research and development project on the ranking of links among these life support systems, this classification will support the process as to specific criteria.

4.0 Links Among Life Support Systems

This part of the report is the heart of the project and presents a structured classification and ranking methodology for links connecting life support networks. The methodology is developed on the links and can later be applied to infrastructure and network ranking. This methodological process is based on the use of ponderable criteria defined with specific ranking goals in mind. The main areas involved in this study have to do with emergency measures.

For any classification exercise to succeed, it is very important to properly define and characterize the things being studied. Thus we first present a definition of the types of links. Then, these links are categorized in terms of content. The ranking methodology developed is then presented, followed by a presentation of the criteria developed. Finally, descriptive criteria parameters are explained along with the ranking scales resulting from them.

4.1 Definition of Links

A link is an interaction between two Life Support Networks (LSNs). This interrelation makes it possible for a vulnerability to be transferred from an origin network to a destination network through infrastructures and/or operations. It has been shown that there are several kinds of links among LSNs, each type having specific characteristics (Robert, 2001, 2002a and 2002b).

Some links are planned. They contribute to the functioning of the various networks. They were desired, thought about, developed and implemented. They are known and taken into account in emergency and mitigation measures. Other links, however, arise from catastrophic events. They are often neglected or ignored in life support network management and in emergency measure planning even though they generate considerable socio-economic impacts (Robert, 2001). It is noteworthy that these links are used to transport materials (water, gas, etc.), services (electricity, transportation, etc.) or computer data. Based on these considerations, three types of links have been identified: direct and indirect links and cyberlinks. They are defined here.

4.1.1 Direct Links

Direct links physically connect two components (infrastructure or operation) of two life support networks (Robert 2002b). Direct links are designed and built intentionally and contribute directly to the proper operation of LSNs. They are thus permanent links. They transport physical materials or services by means of infrastructures. The route of direct links is known.

Examples of direct links: a gas line supplying a thermal electric station, an electric cable powering a water purification plant, a remote flood evacuator control cable.

Direct links can be disrupted or broken. They are involved in the optimal operation of LSNs. They thus cause network failures when they lose their efficiency. It is then harder for networks to fulfill their missions. An attempt must be made to keep them in a proper condition in order to ensure LSN efficiency.

Direct links can be unidirectional or bidirectional (Robert, 2001). Unidirectional links transfer a material or service from an origin network (LSNo) to a destination network (LSNd) while

bidirectional links are used in both directions. Thus, electric power lines may be bidirectional while gas lines are normally unidirectional.

4.1.2 Indirect Links

Indirect links result from network failures. They are not specifically designed or planned but arise from the dispersion of an LSN's material. This dispersion causes changes in the environment in which other networks operate, thus creating a link. Indirect links consist of materials transported from one network to another. Thus, identifying and characterizing such links are based on fundamental notions relating to the material's geography, extension and behaviour.

Examples of indirect links: a hydroelectric dam is submerged and the flood destroys a water plant; a water pipe breaks and the escaping water cuts a gas line; a sewer network backs up and floods a subway station.

It is clear from the preceding examples that to identify these links there must be a context as well as a failure mode. That clearly shows how complex a study of these links is (Robert, 2001). Moreover, these links have a negative connotation since they do not promote the proper operation of networks, but rather are associated with failures. The fact that they are not intentional explains why they are often neglected or even completely ignored in emergency measure planning.

Indirect links are created. In normal times, indirect links do not exist. When a LSN fails and material is dispersed, links result from the dispersion of and changes in this material. When this link to another LSN is created, vulnerability is effectively transferred. There is thus a notion of impermanence and creation time, that is, fundamentally associated with such links.

Indirect links are unidirectional (Robert, 2001). Unidirectional links transfer materials from origin networks (LSNo) to destination networks (LSNd). This perfectly describes the indirect link creation phenomenon described above.

4.1.3 Cyberlinks

Cyberlinks arise from the incorporation of information and communication high technology into industrial and production activities. They are used to transfer data, information and messages using electromagnetic, wave or computer processes. Cyberlinks are created intentionally, but the exact routes of such links are hard to pin down and difficult for the uninitiated to track, if we consider the present computer web.

Examples of cyberlinks: Internet and intranet networks; networked computers, remote control of electric power transformer stations by cell phone.

Cyberlinks can be disrupted or broken. Cyberlinks are particularly sensitive and exposed to malicious acts. They are particularly involved in the functioning of LSNs at the operations and management levels.
Cyberlinks are basically bidirectional. Communications are generally two-way. Thus, failure of such links affect both the origin network (LSNo) and the destination network (LSNd), but the

impacts on them are different and depend on the specific nature of the operations being carried on.

Cyberlinks are very different from direct and indirect links because of their relative intangibility. We have not gone into their particularities in this project, which is limited in terms of resources and time.

4.2 Link Categorization

Two parameters will be used to categorize the various kinds of links: the material transported by the link and the link's permanence in the network. The material transported is important because it defines the link's mission and determines its role in the network. Permanence will be used to determine whether the link is involved in normal operations or if it impedes the proper fulfilment of the LSN's mission.

The material being transported is what is carried or transmitted by the link. This material is sometimes a material: the physical material necessary for the destination network to function properly (water, fuel, gas). It can also be data, which is also a source of operational information. Finally, a link might provide a service (public transportation, electricity).

Link permanence is determined by the fact that the link is involved in the normal operation of a life support network. It thus must be maintained at all times. Links are non-permanent when they arise; when a network fails, they are unable to perform their functions, or they are created for the occasion. An attempt must then be made to prevent such links from being created since they are detrimental to associated networks.

Table 2 summarizes these categorization concepts and shows their application to the three types of links: indirect, direct and cyberlinks.

Table 2 Link categorization criteria and parameters

Criteria	Parameters	Links		
		Indirect	Direct	Cyber
Material transported	Physical material	✓	✓	
	Information/data			✓
	Service		✓	
Link permanence	Permanent (normal)		✓	
	Non-permanent (abnormal)	✓		
	Variable (normal)			✓

4.3 Link Ranking

Ranking should be done using a flexible methodology based on the factual and tangible characterization of the links and incorporating the goals of the study in order to determine what links should be given priority.

In this project, the goals defined are related to the development of emergency measures to deal with potential failures of links among several LSNs. This is a general goal that aims to identify links with similar characteristics in order to be able to group them. Three specific goals have been identified:

- **Link vulnerability** – For a link, vulnerability is determined by its physical characteristics and its place in the environment. Links are more vulnerable if they are likely to fail or to propagate a failure through domino effects. Thus, the more vulnerable a link is, the more essential it is to provide mitigation measures.

- **Impact of link failure** – Knowing and characterizing impacts allows effective emergency plans to be developed to prepare for failures in emergency measures. The extent of potential impacts is thus an important parameter in terms of planning. The greater the impacts of a link failure, the more critical it is to consider this link in emergency plans.

- **Emergency measure management operational potential of links** – Risk communication is a very important aspect of emergency measures. However, we believe that communications mechanisms must be set up as a priority when there is a possibility of effectively and operationally managing a crisis. If, when there is a potential for a link to fail, it is possible to take action in one or the other of the two networks to better manage a crisis resulting from this failure, priority operational communications mechanisms should be set up (Robert, 2002b). The greater the possibility of crisis management action being taken when a link fails, the more essential it is to set up risk communication mechanisms.

These three goals will guide the development of criteria for evaluating the criticality of links among LSNs. However, to determine this level, a comparative scale must be developed so that links with similar characteristics that meet a specific goal can be grouped together. Moreover, for each goal, a criticality level has been defined. It is thus important to quantify criticality levels based on similar features and characteristics.

Following the example of the HSAS (White House, 2002), a quantitative scale for determining how critical links are defined was developed. This determination scale was established using theoretical principles taken from works on expert systems and endorsement theory (Cohen, 1986; Peyrat, 1996; Robert, 1996 and 1998). The concepts used should be universally recognized, which means that data handled must be tangible and precise in order to ensure a proper understanding of the situation. The scale is symbolic.

The scale presented is divided into five criticality levels, each being associated with a definition of the criticality level of the link being studied, based on the chosen goal. Thus we can envisage grouping links into five criticality intervals:

- Extremely critical
- Very critical
- Critical
- Slightly critical
- Very slightly critical

After the analysis has been completed, each link will be included in a criticality interval and will have a numeric scale defining its exact position in this interval. It will then be possible to determine that we wish to process links that are included in a specific interval and then analyze them based on their numeric order. It is then possible to find similarities, particularities, differences and preferred potential courses of action among the links.

4.4 Characterization Criteria

Link classification and then ranking, based on criticality levels for specific goals, requires that descriptive criteria regarding these links be defined. These criteria are then used to characterize the links being studied relative to a goal and to measure how the link meets this goal. Based on this measure, it is possible to determine the level of criticality of the links being studied relative to goals.

These criteria must respect certain principles in order to ensure uniformity and consistency in the criticality evaluation methodology. The basic principles include the notions of granularity, pragmatism, consistency and changeability. These are described as follows:

- **Granularity** – As far as possible, criteria must represent only one piece of information or concept. They must not include a number of different notions.
- **Pragmatism** – Criteria must be tangible and measurable or quantifiable. As far as possible, they must leave no room for subjectivity.
- **Consistency** – Criteria must be consistent with the fields of expertise they cover. Use of very specific criteria regarding expertise with general criteria must be avoided. Moreover, these criteria must be recognized and understandable to all experts in the field.
- **Changeability** – Criteria must be able to evolve as new knowledge is gained. They must therefore be defined and characterized in a general way and not be too specific. Moreover, all criteria must be diversified in order to cover the entire field being studied.

Characterization criteria are divided into three categories associated with three criticality goals. These criteria are briefly named, described and presented. The utilization principle used to rank links based on criticality goals is also presented.

An evaluation grid for each of the criteria may be found in Appendix A.

4.4.1 Link Vulnerability

The first category of criteria is associated with the potential vulnerability of links. The critical points of links must therefore be shown. The criteria associated with this criticality principle must use tangible physical data regarding the links to determine their potential for failure. Since this data is physical, it is relatively easy to obtain by studying the LSNs. System managers should not be asked to assist. Seven characterization criteria are used to show link vulnerability and are discussed here.

Link Nature

Link nature represents the type of link – that is, its role in an LSN's operation. We recognize the existence of direct links, cyberlinks (network operation), and indirect links (LSN failure). The utilization principle states that indirect links are the most vulnerable since they are less well identified and thus less well controlled by network managers. Since indirect links are not part of a network's normal operation but rather arise from its failure, they are often forgotten and then cause domino effects. This criterion was chosen to determine the material transported by the link and its incorporation into the normal operation of the networks.

Geographical Corridor

The geographical corridor is the distance in kilometres over which a link is deployed. The utilization principle states that the longest links are the most vulnerable and thus critical. The distance evaluation scale must be changeable in order to be more adaptable to the particular context of links. This criterion is critical since it shows which LSNs are vulnerable at certain links.

Direction

Link direction pertains to the direction of the material transported by the link. Bidirectional links are more critical than unidirectional links since they allow vulnerability to be transferred to two LSNs. This criterion is used to illustrate the path taken by a link's material and so better determine what infrastructures, critical or not, will be most vulnerable to link failure.

Impregnation

The notion of impregnation refers to the extent to which a failure affects an LSN. Impregnation is designated by the type of component affected by a link: operational or structural. The utilization principle gives priority to operational components since these components are, in the authors' experience, the least considered in terms of emergency measures. They are therefore generally more vulnerable.

Link Protection in Normal Situations

The link protection criterion evaluates each link based on the measures instituted to protect it in normal situations. Links that are not protected are obviously more vulnerable.

Link Mitigation

Link mitigation determines what links are the least well protected in exceptional situations. We must first opt to process links that have no mitigation measures. Indirect links are also given priority because they arise directly when exceptional situations occur and aggravate them.

Associated Vulnerability

Associated vulnerability is the criterion used to evaluate the hazards most likely to affect a link. This criterion favours links that are most able to withstand malicious acts and human error. This choice relates directly to the new concerns of emergency measures officials who believe that computer risks are becoming more and more serious.

4.4.2 Impacts of Link Failure

The second criticality goal used to establish a criteria category is all the impacts that potential failures of a link can have on LSNs. A link's criticality is determined by its ability to deal with failures and by its potential effect on the operation of associated LSNs.

Data describing network operation will be needed to determine the effects of a link failure. This data is technical but usually harder to obtain that that having to do with physical descriptions. System managers can sometimes provide useful assistance.

System Classes

System classes are important in determining the potential impact of a link's failure. Priority must be given to links that connect more critical LSN classes. In this project, LSN classes are not evaluated in terms of criticality. Thus, dummy values will be used, but once an LSN ranking is effective based on similar goals, these results will be incorporated.

Criticality of Affected Components

The managers of the affected networks first determine the criticality of affected components. Priority is to be given to links connecting very critical components. They will have greater impacts on carrying out the missions of the networks in case of failure.

LSN Efficiency

Network efficiency is a measure of changes in a network's efficiency following link failure or the creation of indirect links. This criterion thus evaluates the impacts of the failure or creation of this link on a destination network's operations. Ranking will be done by determining the greatest change in LSN efficiency for the link. The direction of the link, which is used to determine whether it affects only the destination network or also propagates to the origin network, must not be overlooked. This criterion is used to show that networks are interdependent and can no longer fulfill their missions properly if certain interactions are not maintained or avoided.

Potential Domino Effects

This involves evaluating – by means of studies of the impacts of several life support networks – how many domino effects a link can give rise to. A bidirectional link means that the origin and

destination networks must be evaluated. Links causing the greatest number of domino effects on networks should receive priority. The evaluation scale must be adapted based on the total number of LSNs evaluated by the study. It is obvious that this criterion can be used to rank links among LSNs based on their potential for transferring vulnerability impacts to other networks.

Alternative

Link alternative is a criterion that applies to direct links and cyberlinks. Indirect links arise from network failures. They certainly have no alternative. Prioritized links will be those that do not have an alternative that would allow network efficiency to be maintained in case of failure. This criterion was chosen to show the possible resources of LSNs in case of link failure.

4.4.3 Emergency Measures Management Operational Potential of Links

The third criticality goal of links ranks them based on management operational potential when links fail or are created. Links with the greatest potential for improvement at the operational level will be prioritized to optimize their management. It must thus be determined whether a link has an operational potential for concrete action and for instituting mitigation crisis management and risk communication measures.

The data used is associated with life support network management information. This data evolves since it arises from network operation procedures and rules. This information can be obtained from documentation or directly from network managers, who may or may not have considered what measures to take regarding a link. The criteria used will vary, again depending of the goals of the study. Six criteria describe this management potential and are discussed here.

Authority

A link's authority indicates who is responsible for it. Since origin and destination LSNs are often different and thus managed by different administrative entities, it is hard to determine who should be responsible for putting this link in place and maintaining it. Indirect links, which will clearly be less managed by the LSNs since they are unexpected and badly identified, must be given priority. Cyberlinks will also be given priority since they often come under a different authority than the main network. Direct links are much more obvious. Since infrastructures must be maintained regularly, the responsible authority is known. This criterion is so chosen to illustrate what links are most likely to be without any authority responsible for the impacts of link failure and creation, and for managing the emergency measures associated with them.

Preparation

The link preparation criterion attempts to determine whether this link was included in exercises and emergency measures. The principle for evaluating this criterion is that if a link is not given priority in terms of emergency measures, it is critical to remedy that situation. The data used by this criterion is quite simply its incorporation into emergency measures and preparatory exercises.

Risk Communication

This criterion complements the preceding one to the extent that we attempt to show the existence of a structure used to communicate risks for this link. Links that do not have this structure should be given priority in order to optimize their management and emergency measures potential. This criterion was included in the analysis to show that an effective means of communication, whatever it is, must allow networks to react to certain events. It is an important management tool during the prevention and preparation stages, and when reporting that a threat to the link has been detected.

Necessary Reaction Time

Reaction time has to do with the time needed to create an indirect link. Indirect links might take some time to be created, giving a window of opportunity for adequate emergency and mitigation measures to be set up. Thus, priority must be given to links with quite a short creation time and that are hard or impossible to manage. The link's evaluation scale will be expressed in time units, whose precise definition will depend on the particular circumstances. This criterion was chosen to show that not all links allow for optimal management and that more attention must be paid to those that seem more difficult to manage.

Link Operational Management

Link operational management is the criterion used to give priority to links that are manageable, depending on the time available. This criterion will be evaluated based on the time needed to control the failure of a direct link or the time taken to create an indirect link.

Recovery Time

Recovery time is the time needed to put direct links and cyberlinks back in operation. In the case of indirect links, it must be noted that recovery time is characterized by the time needed for the origin and/or destination LSN to regain control of the material carried by the link. Return-to-normal activities can then commence. Links with long recovery times, and thus lesser management potential, will be given priority. Recovery time is used to evaluate how long the impact of a failure will be felt in the networks involved.

4.5 Identification Parameters and Evaluation Scale

It must be possible to characterize, evaluate and measure the criteria defined above in order to compare links and to determine their level of criticality based on study goals. To do this, parameters that are specific to each criterion will be used. Parameters are data that are accessible, with a few exceptions, in most links among LSNs and can be used to determine criticality of the links. After this data has been collected, characterization criteria evaluation scales can be completed. Parameters are thus descriptions of the links, whereas criteria can be used to determine the criticality of the links.

Here then is a list of the parameters identified, in order of criticality principle. We will also show how to collect data and possible assignable values. An inaccessible parameter will often receive a very high value in order not to omit certain things that might prove to be extremely important.

As in the case of criteria, parameter use is very likely to vary over time, depending on LSN diversity. These parameters are described in Appendix B.

Link nature – The nature of the link is determined by two characteristics, both easily identifiable by simple observation of the link's physical characteristics: the element being transported and the permanence of the link. The element being transported can be information or data (cyberlinks), a service (direct links), or a physical substance (direct and indirect links). The permanence of the link distinguishes between direct links (permanent) and indirect links (temporary).

Possible values of the parameter: Indirect/Direct/Cyberlink

Geographical distance – Geographical distance is also a characteristic of a link that can be determined quite easily, particularly in the case of direct links. All that is required is to identify the length of the various links.

Possible values of the parameter: Distance in km

Link direction – Link direction determines, in the case of direct links and cyberlinks, the direction of the material in the link. Links are therefore bidirectional or unidirectional. This information is again available by observing the life support network.

Possible values of the parameter: Unidirectional/Bidirectional

Nature of components – The nature of the components connected by the link can also be determined by physically analyzing the link and its extremities. Components are structural or operational in the network. Origin (LSNo) and destination (LSNd) network components are considered.

Possible values of the parameter for an LSNo: Operational/Infrastructure
Possible values of the parameter for an LSNd: Operational/Infrastructure

Existence of normal protection on the link – Normal protection measures on a link are relatively obvious if they are of a structural nature. However, when they are of an operational nature, it is advisable to consult with network managers to identify them more easily. This parameter does not apply to indirect links since they are created in exceptional situations.

Possible values of the parameter: Yes/No/Unavailable

Existence of protection in exceptional situations – This variable can be found by examining all the links. It must be determined whether exceptional mitigation or protection measures have been established over and above normal protection measures.

Possible values of the parameter: Yes/No/Unavailable

LSN class – The link's origin and destination LSNs must be determined in accordance with the definition of life support network classes.

Possible values of the parameter for an LSNo: A / B / C / D / E
Possible values of the parameter for an LSNd: A / B / C / D / E

Component criticality – Component criticality is determined, along with managers, based on how important the components affected by the link are to the proper operation of a network. These criticality values are evaluated according to a symbolic scale used to determine various criticality levels.

Possible values of the origin component parameter: Extremely critical / Very critical / Critical / Slightly critical / Very slightly critical
Possible values of the destination component parameter: Extremely critical / Very critical / Critical / Slightly critical / Very slightly critical

Reduction in efficiency (RE) – This parameter measures the loss of origin (LSNo) and destination (LSNd) network efficiency following the failure or breakage of a link. This loss is expressed as a percentage. This calculation can only be done in collaboration with the managers of both networks affected by the link.

Possible values of the parameter for an LSNo: % reduction in efficiency
Possible values of the parameter for an LSNd: % reduction in efficiency

Networks linked to the affected component – This information on network operation can be evaluated by observing the LSNs. It must be determined how many other networks are connected to the network component affected by the link. This parameter is evaluated for both the origin (LSNo) and destination (LSNd) networks.

Possible values of the parameter for an LSNo: Number greater than or equal to 0
Possible values of the parameter for an LSNd: Number greater than or equal to 0

Existence of an alternative to the link – This information cannot be obtained without the support of the LSN managers. An alternative is a means of maintaining LSN efficiency even after a failure occurs. The evaluation scale must therefore determine whether the link has an alternative or not, or whether this information is inaccessible. Indirect links never have alternatives.

Possible values of the parameter: Yes / No / Unavailable / Inapplicable

Existence of emergency measures – This parameter is evaluated by determining, with the assistance of managers, whether a link is specifically included in emergency plans. It is evaluated for both the origin (LSNo) and destination (LSNd) networks.

Possible values of the LSNo parameter: Yes / No / Unavailable
Possible values of the LSNd parameter: Yes / No / Unavailable

Existence of preparatory exercises – This parameter is evaluated by determining, with the assistance of managers, whether a link was already covered in certain exercises.

Possible values of the parameter: Yes / No / Unavailable

Existence of a communications structure – Communications structures are identified with the assistance of network managers.

Possible values of the parameter: Yes / No / Unavailable

Link reaction time – This parameter applies only to indirect links. It is defined using vulnerability and impact studies. It measures the time needed to completely deploy a link (during creation).

Possible values of the parameter: Time (in minutes / hours / days) / Inapplicable

Operational management time – Operational management time can be identified for direct links, cyberlinks and indirect links. This parameter determines whether operational management is possible in one or both networks.

Possible values of the parameter: Yes / No / Unavailable

Recovery time – This parameter indicates how much time is needed to re-establish a link or regain control of a situation in the case of indirect links. This data can be taken from LSN impact or vulnerability studies. The symbolic time measurement values (short, medium, long or minutes, hours, days) are associated with numeric values.

Possible values of the parameter: Time (in minutes / hours / days)

5.0 Ranking Methodology

The ranking methodology is simple and involves calculations. By assigning a value to each parameter, a weight to each criterion and a coefficient at the criticality class level, it is possible to "calculate" a link's criticality. The numeric results are then represented qualitatively based on the criticality scale previously defined.

This approach is designed to be flexible and users must be able to intervene in the calculation method in order to situate the results based on study goals. The calculation method must therefore be modular, understandable and simple.

The methodology is presented in general, and application to the strict framework of this project is described to facilitate comprehension.

5.1 Criticality Classes

Criticality classes correspond directly to criticality goals. A weight is associated with these classes to give greater versatility to the process by favouring certain goals over others. It should be noted that a null weight means that a goal is not considered.

- Number of classes: n
- Application: n = 3
    - Class 1: link vulnerability
    - Class 2: impact of link failure
    - Class 3: link's emergency measures management operational potential

- Weight of a class of criteria: Pcl_j, where j = 1, n
- Weights range from 0 to 5. A weight of 0 indicates that this class is not considered in the study.
- Application: by default, the weight always equals 1
    - Class 1: $Pcl_1 = 1$
    - Class 2: $Pcl_2 = 1$
    - Class 3: $Pcl_3 = 1$

5.2 Characterization Criteria

Characterization criteria are associated with a specific criticality class. For each criticality class, there are m criteria.

- Application:
  - Class 1 = Link vulnerability
    m = 7 Criterion
    1: Link nature
    2: Geographical corridor
    3: Direction
    4: Impregnation
    5: Link protection in normal situations
    6: Mitigation
    7: Associated vulnerabilities
  - Class 2 = Impacts
    m = 5 Criterion
    1: Network classes
    2: Component criticality
    3: Network efficiency
    4: Potential domino effects
    5: Alternative to the link
  - Class 3 = Operational management and emergency measures
    m = 6 Criterion
    1: Authority
    2: Preparation
    3: Risk communication
    4: Link reaction time
    5: Link operational management
    6: Recovery time

- Each criterion (i) of a class (j) has a weight = Pc_{ij}, where i = 1, m and j = 1, n
  - The weights of the criteria also range from 1 to 5. A weight of 0 indicates that this criterion is not used in the study.
  - Application: By default, criteria weights are always set to 1 for all the criteria.
  - Example: Class 1: Vulnerability
    Criterion 2: Geographical corridor
    Criterion weight: $Pc_{21} = 1$

5.3 Methodology

- Each link is analyzed in turn.
- For each link, each of the criticality classes is analyzed in turn.
- For each link and each class, each criterion for this class is analyzed in turn.
- For each specific criterion, the link being studied is evaluated and a value between 1 and 5 is assigned to it based on the use principle set forth in Appendix A.
- This value for a specific link is noted:

- Cvlink $_{ij}$,where i =1, m; j = 1, n
- This is the value of the link being studied for criterion i of class j.

- Since each criterion and each class have different weights, the total value of the link being studied is thus obtained using Equation 1:

Equation 1

$$VT_{link} = \sum_{j=1}^{n}\left[Pcl_j * \left(\sum_{i=1}^{m} \left(Pc_{ij} * Vclink_{ij} \right) \right) \right]$$

All the links studied get a value that depends on the values assigned to the criteria, the weights of the criteria, and finally the weight of the class. It is now possible to rank the links since they are all categorized then ordered according to a particular value. Ranking is done in decreasing link value order.

- Since some links among life support networks can have similar characteristics, it is useful to group these links by interval. Based on criteria evaluation scales, five criticality intervals are defined. These intervals are calculated based on the maximum possible value of a link. This maximum possible value arises from weights assigned to the criticality classes and to the criteria.

- In the case of a criteria evaluation scale ranging from 1 to 5, this maximum value is calculated below using Equation 2, knowing that 5 is the maximum value that each of the criteria can take on according to the evaluation grids:

Equation 2

$$ValMax = \sum_{j=1}^{n} Pcl_j * \left(\sum_{i=1}^{m} \left(Pc_{ij} * 5 \right) \right)$$

- The interval limits are then defined as follows:
  - Bi = MaxVal / 5

- The intervals are defined numerically and colours can be associated with them, taking into account the criticality scale defined above:

Interval 1 = [0;*Bi*]
Interval 2 =]*Bi*;2*Bi*]
Interval 3 =]2*Bi*;3*Bi*]
Interval 4 =]3*Bi*;4*Bi*]
Interval 5 =]4*Bi*;5*Bi*]

Interval 1 = correspondence with respect to criticality*: very slightly critical (blue)*

Interval 2 = correspondence with respect to criticality*: slightly critical (green)*

Interval 3 = correspondence with respect to criticality*: critical (yellow)*

Interval 4 = correspondence with respect to criticality*: very critical (orange)*

Interval 5 = correspondence with respect to criticality*: extremely critical (red)*

Thus, each link is associated with an interval, a colour and a description of its criticality. Although the colour scale is not used in this report, it can be effective in graphical representations. Once the link processing order has been established, the only thing left to do is to put means of action in place to ensure that each link is considered and processed based on its particular characteristics.

6.0 Application

The process presented above must allow links among life support networks to be ranked in a standard manner by standardizing the data used and its interpretation. This is necessary to successfully limit the subjectivity of ranking activities. Standardizing this process should make it easier for all those involved to understand what is going on. The methodology can then support the taking of joint action. It will be shown that by using tangible and measurable criteria, it is possible to compare links of different kinds and to rank them in a quantified manner. A calculation example showing how the method is applied to study links is presented along with a compilation of all the results obtained for all links. Following this, a number of ranking possibilities (and not just one) are presented. We also show that ranking differs depending on the goals considered, the results supporting the concept of variable criticality. The ranking methodology is made clear through a study of the five links below. A description of each link is given in Appendix B.

- **Link 1** – Telephone link between a municipality's fire and police departments. It is used to transfer information and to coordinate emergency and security teams. This is a cyberlink.
- **Link 2** – Electric power distribution wire supporting the activities of a municipality's water purification plant. This link is direct.
- **Link 3** – Link between an automated computerized control network and electric power production facilities. This is a cyberlink.
- **Link 4** – Potential indirect link between an oil pipeline and a water pipe. This link is indirect.
- **Link 5** – Link providing electric power to a subway network. This link is direct.

The choice of different kinds of links shows that the method applies to direct and indirect links as well as to cyberlinks.

6.1 Calculation Example

For a given link, the procedure to be followed to determine the value of each criterion (Cvlink) and to obtain the total value of the link (Tvlink) is presented hereunder. The calculations are explained in detail in Appendix C.

Link 1 will be used as an example to illustrate the methodological steps, which are:

1. Calculation of the value of each criterion;
2. Calculation of the link's total value (Equation 1);
3. Calculation of the link's maximum value (Equation 2); and
4. Determination of the limits of the criticality levels.

Table 1 shows the detailed results of these calculations for Link 1.

Table 3 Calculation of the value of Link 1

GOAL 1: Link vulnerability		**GOAL 2: Impacts of link failure**		**GOAL 3: Emergency measures management operational potential**	
Criteria	**Value**	**Criteria**	**Value**	**Criteria**	**Value**
Cvlink 1: Link nature = cyberlink	3	Cvlink 8: Network classes = 2 class E LSNs	3	Cvlink 13: Authority = Cyberlink	5
Cvlink 2 Geographical corridor = 0.5km	1	Cvlink 9: Criticality of affected components = 2 extr. crit. comp.	5	Cvlink 14: Preparation = IEMO = unav., IEMD = unav., IPE = unav.	5
Cvlink 3: Direction = Bidirectional	4	Cvlink 10: LSN efficiency = LSNo 90% and LSNd 70%	4	Cvlink 15: Risk communication = no	5
Cvlink 4: Impregnation = affects 2 operations comp.	5	Cvlink 11: Potential domino effects = bidirectional and NNCo + NNCd = 4	5	Cvlink 16: Reaction time = Inapplicable	0
Cvlink 5: Protection in normal situations = no	5	CVlink 12: Alternative = no	5	Cvlink 17: Operational management = no	1
Cvlink 6: Mitigation = yes	1			Cvlink 18: Recovery time = 2 hrs.	4
Cvlink 7: Associated vulnerabilities = LSNo and LSNd comp. are operational	5				
Total value goal 1	**24**	**Total value goal 2**	**22**	**Total value goal 3**	**20**
Maximum value goal 1 7*5 = 35		Maximum value goal 2 5*5 = 25		Maximum value goal 3 6*5 = 35	
Maximum value of link 18*5 = **90** (calculated using Equation 2)			Total value of link 1: 24+22+20 = **66** (calculated using Equation 1)		

Abbreviations:
Comp.: component
LSNo: origin life support network
LSNd: destination life support network
Extr. Crit.: Extremely critical
NNCo: Number of networks connected to the origin component
NNCd: Number of networks connected to the destination component
IEMO: Importance attached to emergency measures in the LSNo
IEMD: Importance attached to emergency measures in the LSNd
IPE: Importance attached to preparatory exercises
Unav.: Unavailable

To define the range of the intervals, we divide the maximum value by five (which is the maximum value for a criterion).

Bi = 90/5 = 18

For Link 1, the criticality level intervals are:

- Interval 1: Very slightly critical = [0, 18]
- Interval 2: Slightly critical =]18, 36]
- Interval 3: Critical =]36, 54]
- Interval 4: Very critical =]54, 72]
- Interval 5: Extremely critical =]72, 90]

Since Link 1 received a total of 66, it is in Interval 4 – very critical.

The results for each link are given in Table 4.

Table 4 Values obtained for the five links

Links	Goal 1	Goal 2	Goal 3	Total value
1	24	22	20	**66**
2	12	18	19	**49**
3	24	11	17	**52**
4	12	12	28	**52**
5	10	15	9	**34**

6.2 Interpretation of Results

6.2.1 Ranking Possibilities

Once the results have been obtained, the links can be ranked by combining the values of several goals or analyzing the results prioritizing a single goal. It must be remembered that criticality levels mean little if they are not related to the goals identified previously, that is:

- **Goal 1**: Establish mitigation measures by identifying the most vulnerable links.
- **Goal 2**: Improve emergency measures planning by identifying the links whose failure would cause the greatest impacts.
- **Goal 3**: Optimize crisis management by identifying links with the best management operational potential.

Using the results of all the links for each goal, there are several ranking possibilities. The tables below show the levels and the criticality intervals obtained for the five links being studied. The results are first presented separately for each goal. The results for Goals 1 and 2 are then combined since it is useful to analyze criticality by combining vulnerabilities and impacts. Finally, the result of the total value of the link is obtained by adding the results of the three goals. Table 5 summarizes the intervals obtained and Table 6 shows the criticality levels obtained for each link. Table 7 is based on the data in Table 6 and shows the rankings obtained.

Table 5 Criticality Level Intervals

Criticality levels	**Goal 1**	**Goal 2**	**Goal 3**	**Goals 1+2**	**Goals 1+2+3**
Very slightly critical	[0;7]	[0;5]	[0;6]	[0,12]	[0;18]
Slightly critical	]7;14]	]5;10]	]6;12]	]12;24]	]18;36]
Critical	]14;21]	]10;15]	]12;18]	]24;36]	]36;54]
Very critical	]21;28]	]15;20]	]18;24]	]36;48]	]54;72]
Extremely critical	]28;35]	]20;25]	]24;30]	]48;60]	]72;90]

Table 6 Criticality of links by goals

Links	**Goal 1**	**Goal 2**	**Goal 3**	**Goals 1+2**	**Goals 1+2+3**
1	Very critical	Extremely critical	Very critical	Very critical	Very critical
2	Slightly critical	Very critical	Very critical	Critical	Critical
3	Very critical	Critical	Critical	Critical	Critical
4	Slightly critical	Critical	Extremely critical	Slightly critical	Critical
5	Slightly critical	Critical	Slightly critical	Critical	Slightly critical

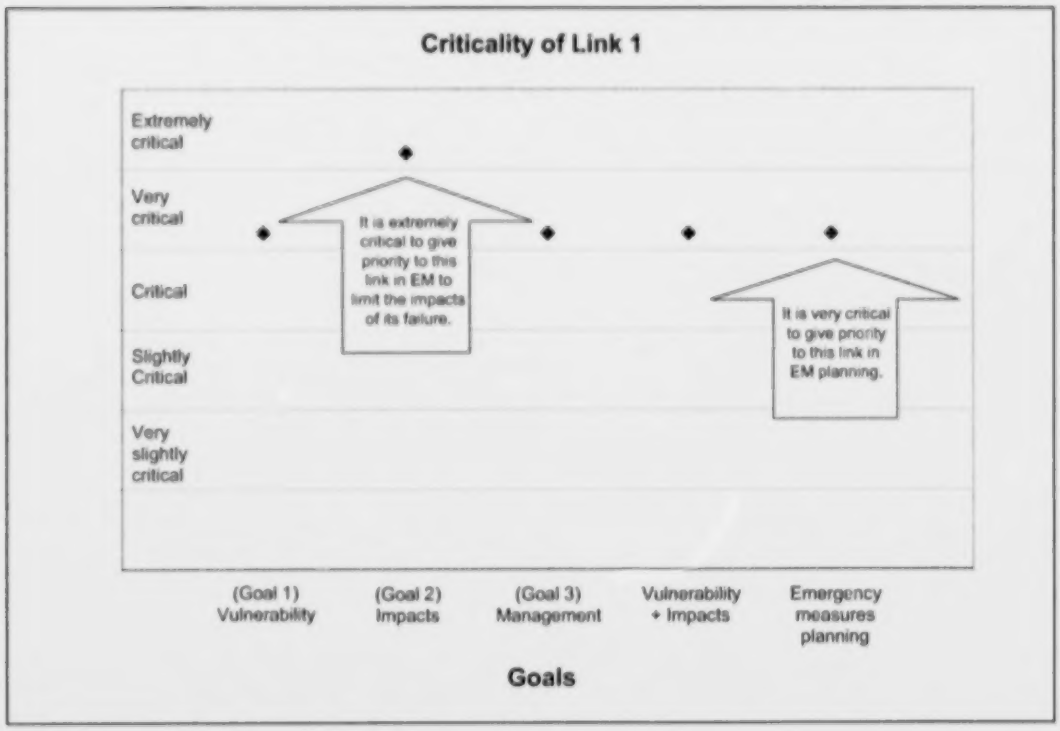
Table 7 Ranking of links by goals

Goal 1	Goal 2	Goal 3	Goals 1+2	Goals 1+2+3
1, 3	1	4	1	1
	2	1, 2	2, 3, 5	2, 3, 4
2, 4, 5	3, 4, 5	3		
		5	4	5

The first step in analyzing Table 6 is to give a meaning to the criticality levels obtained by each link. As was mentioned above, the results cannot be interpreted apart from the goals. The results of Link 1 demonstrate this principle. The result obtained for Goal 1 places it in the very critical interval. However, this result must not be considered as an absolute value but rather the question must be asked: how is this link **very critical** to achieving this goal?

Since Goal 1 refers to link vulnerability, the result means that to reduce the vulnerability of this link, it is **very critical** to institute mitigation measures. For the second goal, which refers to the impact of a link's failure, the result implies that it is **extremely critical** to consider Link 1 in emergency plans to limit the impacts implied by a failure of this link. For the third goal, which refers to emergency measures management operational potential, the result means that it is **very critical** to give priority to this link since its high operational potential makes it possible to optimize management during a crisis. It is also possible to combine the results of Goals 1 and 2. This result might be useful in identifying links that are vulnerable and whose failure might give rise to significant impacts. This being so, it is **very critical** to give priority to Link 1. In addition, the results of the total value of the link can be used in general emergency measures planning. Again, the result does not literally mean that Link 1 is very critical. Although it is very critical to give priority to this link when planning and implementing emergency measures, it does not mean that it is very critical in itself. Criticality must be seen relative to goals. Figure 1 might help explain this interpretation of results.

Figure 1 Criticality of Link 1


Criticality of Link 1
Extremely critical
Very critical
Critical
Slightly Critical
Very slightly critical
It is extremely critical to give priority to this link in EM to limit the impacts of its failure.
It is very critical to give priority to this link in EM planning.
(Goal 1) Vulnerability
(Goal 2) Impacts
(Goal 3) Management
Vulnerability + Impacts
Emergency measures planning
Goals

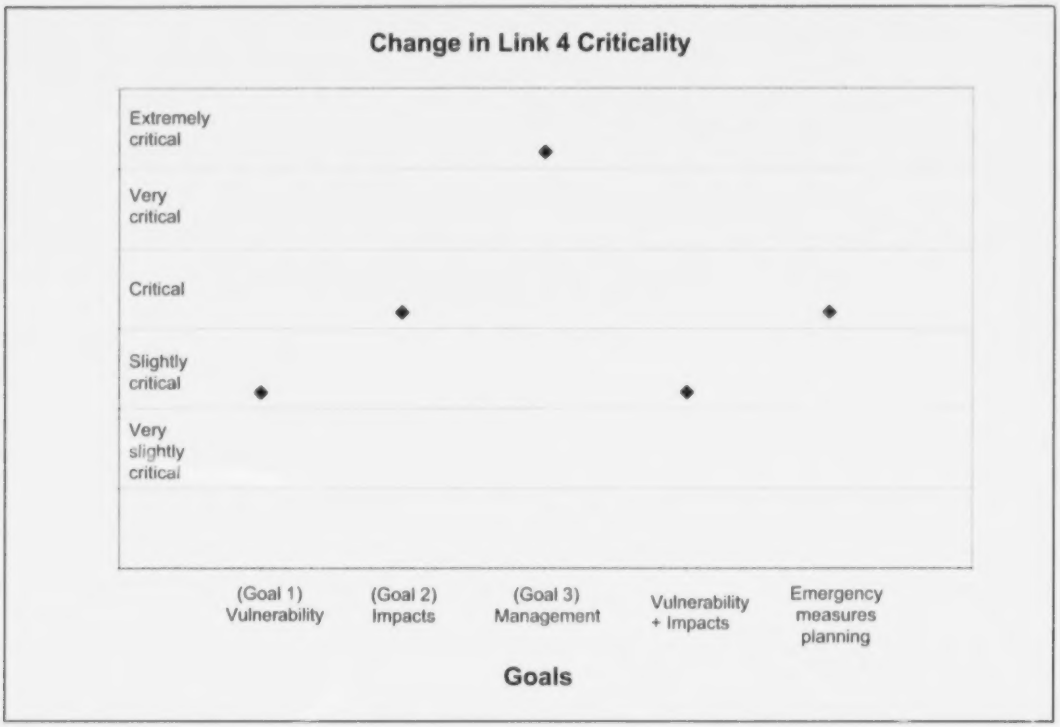
The results shown in Table 6 allow the links studied to be prioritized by considering one or more goals. It is possible to study a single link as was shown above or to compare several links to find out which ones to prioritize based on the goals to be achieved. By looking at the results obtained in Table 6 for Goal 2, we can conclude that Link 1 should be given priority in order to reduce potential impacts in case of failure.

It must be considered that the greater the number of goals used, the less significant the results will be from an operational point of view and vice-versa. That is, an analysis focused on a single goal will give results that can be more easily applied in a practical way. The results can then be interpreted as indicators of the direction to take to achieve the intended goal. A study that combines several goals will however give a more general view, which might be necessary when planning large-scale emergency measures. This can be seen in the rankings shown in Table 7 (see also Figure 2). If only Goal 3 is studied, Link 4 is the first link to be prioritized. However, if Goals 1 and 2 are added, it seems to lose its importance. It is therefore essential to correctly define the goals to be achieved during ranking to avoid "forgetting" links that are needed to achieve them.

6.2.2 Variations in Criticality Levels

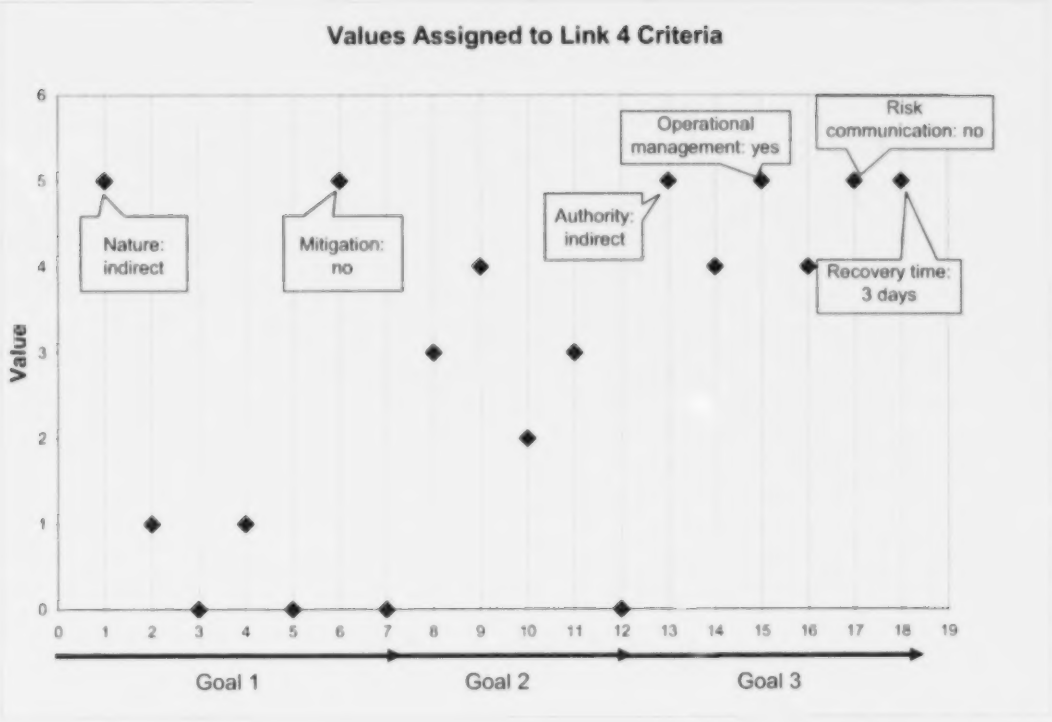
According to Table 6, criticality levels vary depending on the goals for a single link. This can be explained by the simple fact that each goal is based on different criteria and emphasizes different data. Link 4 is a good example of variation in criticality levels to make this principle clear. This variation can be seen in Figure 2.

Figure 2 Change in Link 4 Criticality



Depending on goals aimed at, its criticality level varies from slightly critical to extremely critical. These variations can be explained by discrepancies in the values assigned to the criteria represented in Figure 3.

Figure 3 Values Assigned to Link 4 Criteria



These variations might be indicators of the link's strong and weak points. For example, for the vulnerability goal, there are only two criteria that get a maximum of 5. Since the other criteria have low values, we might conclude that Link 4 is not very vulnerable. It is for the criteria of Goal 3 that the greatest numbers of maximum values were assigned. For example, there is no risk communication system to help in managing this potential link. This indicates a weakness that might be remedied by taking concrete action. Variations in criticality can thus be analyzed individually depending on users' needs. In the graphs presented above, it was shown that the results obtained with this method could be represented in various ways. This benefit of the method can be exploited to facilitate understanding of what is at stake, particularly in a multidisciplinary work situation.

6.3 Method Uses

The method presented has many uses. It allows us to limit subjectivity when ranking LSNs while allowing us to explain the procedure followed. By presenting the results in the form of simple graphs, we ensure a better understanding of the issues by all those involved in planning emergency measures. By standardizing data processing, it is also possible to improve information transfer. This method is also flexible, which allows users to adapt it to their own needs. New criteria can be added if they meet the requirements listed above. This method can be considered as a tool that helps with decision-making in emergency measures planning. It does

not give specific guidelines or actions to take, but rather sheds light on what links should be given priority. It can play the role of a compass for managers planning emergency measures by indicating the direction in which to go to achieve the intended goals.

7.0 Conclusion

The presented ranking process shows the possibility of developing a comprehensive methodology for studying vulnerability and risk with the aim of reducing domino effects. However, this is possible only if the guidelines set forth in the preceding chapters aimed at reducing subjectivity and promoting consistency and pragmatism during ranking activities are applied.

It has been established that to reduce subjectivity, we must first define the notion of criticality so that it can be evaluated rigorously. A first step in this direction was made by showing that criticality is a variable that must be relativized, among other things, as it relates to the goals of ranking. The definition of criticality must be refined still more if the goal is to be able to apply it to the ranking of a network's components or to complete networks. It is however possible to conclude that studying and evaluating it must be done using tangible and measurable parameters in order to limit subjectivity during the process. A single pragmatic conception of criticality and its evaluation is necessary to incorporate data from several networks into a comprehensive study of LSNs. The multidisciplinary aspect implied by a study of domino effects requires that subjectivity be limited in order to improve emergency measure planning by ranking critical infrastructures in a way that is meaningful for all those involved.

Once subjectivity has been limited, it is possible to standardize the ranking process. Before starting the ranking, we must ensure that there is a single study framework that is clearly defined. Although it remains to be completed, the definition of LSN classes will be useful in applying the methodology to a more general study of LSNs. Standardization of ranking studies also requires the use of a flexible method that can be adapted not only to links and their components but to networks of different kinds. The flexibility of the method developed was shown by the various possibilities for using it and by the changes that users can make with it. However, the requirements must be met when choosing criteria so that they remain tangible and measurable. If these principles are followed, subjectivity can be reduced and standardization maintained in the process. This also makes it possible to standardize the representation of data and results, thus improving information transfer. Standardizing information transfer is all the more important from the point of view of a comprehensive methodology. It facilitates participation and comprehension by everyone involved in emergency measure planning that must be multidisciplinary if actions are to be supported by a common direction.

Given the limitations of the study in terms of resources and time, some items have not been discussed in depth. The work involved in this project has confirmed the importance of studying cyberlinks and their particularities in depth. They are becoming more and more common in all types of LSNs, which implies major impacts when failures or malicious acts occur. Thus, not all of the possibilities of the method presented have been explored. The notion of weights that can be assigned to the criteria must be delved into further. It should increase the flexibility of the method by allowing each user to adapt it to his or her needs while continuing to limit its subjectivity. Certain subjectivity-related limits are, however, seen when interpreting the results presented in Table 7. This table shows the tendency of the methodology to group links with similar characteristics together since it uses intervals. While not having the precision of a numerical scale, this method has the advantage of giving as much importance to links that only

had one or two points difference in their total value. Users must, however, make choices concerning processing priorities and these choices may give rise to subjectivity. However, this is limited by the preceding steps, particularly by the use or creation of criteria based on rigorous requirements. In addition to the need to take care in choosing criteria, users must also make choices regarding the links to be studied. Some infrastructures might be served by a large number of links. Procedures must therefore be established to filter and thus differentiate among main and secondary links. Studies can then be done on a realistic scale since it is sometimes technically impossible to analyze all links.

As mentioned above, the notion of criticality must be better defined. The same goes for other concepts having to do with ranking such as vulnerability or criticality classes. A rigorous approach to definition and terminology must thus be taken even before continuing the development of a comprehensive ranking methodology. It will then be possible to rank network classes, LSNs, infrastructures and components based on unique principles. Although that requires a large-scale study, its benefits for all Canadian society are clear. Network managers would then have an in-depth knowledge of domino effects among LSNs and their impacts, while improving knowledge of their own networks. Incorporating such a methodology into studies on LSN risks would make it possible to improve the emergency measures established to deal with internal or external failures and to establish operational mechanisms for communicating risks and vulnerabilities among LSNs.

8.0 Bibliography

Allen H. (1997). «Making a business of dam safety». *International Water Power Dam Construction*, 49(8), p. 20-21.

Bureau de la protection des infrastructures essentielles et de la protection civile. (2001). «Article documentaire – Nouvelle optique pour la gestion des catastrophes au Canada», [en ligne] p.10-14. http://www.ocipep.gc.ca/publicinfo/ep_digest/js_2001/js_2001_fea1_f.html and http://www.ocipep-bpiepc.gc.ca/critical/index_f.html

Can/Csa, (1991). «Risk Analysis Requirement and Guidelines : quality management». *A national standard for Canada*. Conseil canadien des normes, Association canadienne de normalisation, CAN-CSA Q850, Ottawa, 49 p.

Cohen P.R. (1986). *Heuristic reasoning about uncertainty: an artificial intelligence approach*. U.S.A: Pitman publishing inc. 267 p.

Denis H. (1998). *Comprendre et gérer les risques sociotechnologiques majeurs*. Montréal: Éditions de l'École Polytechnique de Montréal, 342 p.

Denis H. (2002). *La réponse aux catastrophes, quand l'impossible survient*. Montréal: Presses Internationales Polytechnique,. 318 p.

Hubbert G., Ledoux B. (1999). *Le coût du risque... L'évaluation des impacts socio-économiques des inondations*. Paris: Presses de l'École Nationale des Ponts et Chaussées, 232 p.

Isenberg J. (1991). «Performance of lifeline and emergency response in Watsonville, CA, to Loma Prieta earthquake». *Proceedings of 4th U.S. Workshop Earthquake Disaster Prevention Lifeline System*, p. 381-390.

Lau D.L. et al. (1995). «Performance of lifeline during the 1994 Northridge earthquake». *CJCE*, 22(2), p. 438-451.

Lemperiere F. (1999). «Risk analysis : What sort should be applied and to which dams ?». *International Journal of Hydropower Dams*, 6(4), p. 128-132.

Miller B. (1999). «The great ice storm of January 1998».. *Workshop on Utility Poles*. Gainesville, Florida, U.S.A.

Moses F. (1998). «Probabilistic-based structural specifications». *Risk Analysis*, 18(4), p. 445-454.

NERC (2002a). «The Electricity Sector Response to The Critical Infrastructure Protection Challenge». *Technical report*, North American Electric Reliability Council, May.

NERC (2002b). «Vulnerability and Risk Assessment». *Technical report*, North American Electric Reliability Council, June.

O'Leary S. (1997). «Concrete rehabilitation for dams». *Proceedings of International Conference Hydropower*, p. 1610-1622.

Plate E.J. (1996). «*Dams and safety management at downstream valleys*». Proceedings International NATO Workshop Dams Safety Manage Downstream valley, *p.27-43*.

Peyrat M., Robert B. (1996). «Knowledge quality and risk management; application: environmental management». *11e International Conference, Applications of Artificial Intelligence in Engineering*, Clearwater, Florida, U.S.A, September 11-13.

President's Comission on Critical Infrastructure Protection. (1997). *Infrastructure Protecting Solutions Catalog*, 1997, Washington, 53 p.

President's Comission on Critical Infrastructure Protection. (1998). *Critical Foundations Protecting America's Infrastructures*, 1997, Washington, 46 p.

http://www.info-sec.com/pccip/web/index.html.

Québec (1999). «Pour affronter l'imprévisible : les enseignements du verglas de '98». *Rapport de la commission scientifique et technique chargée d'analyser les événements relatifs à la tempête du verglas survenue du 5 au 9 janvier 1998. Rapport principal.* Québec : Les Publications du Québec.

Robert, B., Gamelin, C., Hausler, R., Jarry, V. (1996). «Training Concept for Environmental Emergency Measurea : Structuring Kknowledge», *Journal of Contingencies and Crisis Management*, vol. 4, no. 3, p. 175-183.

Robert B., Forget S., Hausler R (1998). «New approach for preparedness evaluation for emergency response». *XIV^e congrès mondial de sociologie; Session sur la recherche canadienne en mesures d'urgence*. Montréal, 26 juillet au 1^er août 1998.

Robert B. (2001). «A Method for the Study of Cascading Effects Within Lifeline Networks». *Workshop on Mitigating the Vulnerability of Critical Infrastructures to Catastrophic Failures*. Alexandria (U.S.A), September 10-11. http://www.ari.vt.edu/workshop/

Robert B. (2002a). «Étude des risques et des effets domino produits par la défaillance d'un aménagement hydroélectrique». *Proceedings of Annual Conference of the Canadian Society for Civil Engineering*, juin.

Robert, B. (2002b). «A new structural approach for the study of domino effects between life support networks». *The Disaster Risk Management Working Paper Series*. World Bank, sous presses.

Selcuk A.S., Semih Y.M. (1999). «Reliability of lifeline networks under seismic hazard». *Reliability Engineering System Safety*, 65(3), p. 213-227.

SEVESO (2000) «Réglementation sur la directive SEVESO II"». Direction des risques chimiques. Inspection technique de l'administration de la sécurité du travail du Ministère fédéral de l'Emploi et du Travail. Belgique. Janvier. http://meta.fgov.be/pm/pmc/frmc17.htm .

Stedinger, J.R., Heath D.C., Thompson, K. (1996). «Risk Analysis for Dam Safety Evaluation : hydrologic risk». *Institute of Water Resources*, Report No. 96-13-16, 51 p.

White House. (2002) Homeland Security Advisory System Presidential Directive-3, [en ligne] p.1-5.
http://www.whitehouse.gov/news/2002/03/print/20020312-5.html and
http://www.whitehouse.gov/homeland/images/300-HSAS-Chart.jpg.

Appendix A – Link Characterization Grid

This appendix gives the characteristics of all the criteria defined in this study in the standardized form of one criterion per page. The contents of this appendix can thus be used directly to rank links.

Criterion Assessment Grid

Criterion name: Nature

Criticality principle: Vulnerability

Utilization principle: Prioritize links that are less easily identified and controlled by the networks.

Comments:

- Indirect links are very vulnerable since they are not clearly identified.
- Cyberlinks are vulnerable since, although they can be identified, they are not under the control of the networks.
- Direct links are the least vulnerable since they are known and controlled by the networks.

Weight of the criterion in ranking calculations: 1

Parameter used: Nature

Scale and law:

- Indirect links must be given priority since they are less well identified and controlled, and thus more vulnerable.

	Nature		
	I	**C**	**D**
Cvlink	5	3	1

Abbreviations:

Cvlink	Criterion value for the link being studied
I	Indirect link
D	Direct link
C	Cyberlink

Criterion Assessment Grid

Criterion name: Geographical corridor

Criticality principle: Vulnerability

Utilization principle: Prioritize links covering large geographical areas.

Comments:

- This criterion applies mostly to direct links and cyberlinks.
- Direct links will probably cover smaller areas.
- In terms of vulnerability, longer links are more exposed.
- Sources of failure can differ between the origin and destination networks. These differences are often not taken into account.
- The proposed distances must be related to regional particularities.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Geographical area (in km) between LSNo and LSNd

Scale and law:

- The longer the links are, the more vulnerable they are.

Geographical corridor			
	Geographical area		
	L ≥ 50 km	**2 km ≤ L > 50 km**	**2 km > L**
Cvlink	5	3	1

Abbreviations:

Cvlink Criterion value for the link being studied
L Link length (in km)

Criterion Assessment Grid

Criterion name: Direction

Criticality principle: Vulnerability

Utilization principle: Prioritize bidirectional links.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Direction
- Nature

Scale and law:

- Bidirectional links are more vulnerable since they affect two networks.
- Indirect links are automatically unidirectional – the second link is then counted.

Link direction	**Cvlink**
Direction: Bidirectional Nature: Direct or Cyberlink	4
Direction: Unidirectional Nature: Direct or Cyberlink	2
Direction: Unidirectional Nature: Indirect	0

Abbreviations:

Cvlink Criterion value for the link being studied

Criterion Assessment Grid

Criterion name: Impregnation

Criticality principle: Vulnerability

Utilization principle: Give priority to links associated with the operational functioning of the network since they are more vulnerable to malicious acts and human error.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Nature of LSNo components affected
- Nature of LSNd components affected

Scale and law:

- The more a link affects an operation, the more vulnerable and hard it is to study because human reliability is involved.

Impregnation		
LSNo	**LSNd**	**Cvlink**
O	O	5
O	I	3
I	O	3
I	I	1

Abbreviations:

LSNo	Origin life support network
LSNd	Destination life support network
Cvlink	Value of the link for the criterion
O	Operation type component
I	Infrastructure type component

Criterion Assessment Grid

Criterion name: Protection in normal situations

Criticality principle: Vulnerability

Utilization principle: Give priority to unprotected links.

Comments:

- Cyberlinks are given priority since they are more vulnerable to malicious acts and human errors.
- Indirect links automatically have a value of zero since they do not exist in normal situations.
- Inaccessible information is considered as potentially missing.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Nature
- Existence of normal protection

Scale and law:

- The least protected cyberlinks are the most vulnerable.

Normal protection		
Protection	**Nature**	**Cvlink**
Yes	D	1
	C	2
No	D	3
	C	5
Unavailable	D	2
	C	4
	I	0

Abbreviations:

Cvlink	Criterion value for the link being studied
I	Indirect link
D	Direct link
C	Cyberlink

Criterion Assessment Grid

Criterion name: Mitigation

Criticality principle: Vulnerability

Utilization principle: Give priority to links without protection measures in the case of exceptional situation management.

Comments:

- Indirect links must be given priority since they arise from and give rise to exceptional situations.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Nature
- Existence of protection in exceptional situations

Scale and law:

- The less protected a link is, the more vulnerable it is. Indirect links are given priority.

Exceptional protection		
	Nature	**Cvlink**
Yes	D or C	1
	I	2
No	D or C	3
	I	5
Unavailable	D or C	2
	I	4

Abbreviations:

Cvlink	Criterion value for the link being studied
I	Indirect link
D	Direct link
C	Cyberlink

Criterion Assessment Grid

Criterion name: Associated vulnerabilities

Criticality principle: Vulnerability

Utilization principle: Give priority to links that are more vulnerable to human error or malicious acts.

Comments:

- Cyberlinks are more vulnerable since they affect more operations.
- In the case of bidirectional links, the origin network becomes a new destination network.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Nature
- Nature of components involved in an LSNo
- Nature of components involved in an LSNd
- Direction

Scale and law:

- Cyberlinks are more vulnerable.
- The operations involved represent greater sources of vulnerability.

Cvlink based on associated vulnerabilities							
LSNo	LSNd	Nature					
		Link Direct		Cyberlink		Indirect Link	
		Uni	Bi	Uni	Bi	Uni	Bi
I	I	1	1	2	2	0	0
I	O	3	3	4	4	1	1
O	I	2	3	3	4	1	1
O	O	4	4	5	5	2	2

Abbreviations:

Cvlink	Criterion value for the link being studied
I	Infrastructure
O	Operation
LSNo	Origin life support network
LSNd	Destination life support network
Uni	Link direction: unidirectional
Bi	Link direction: bidirectional

Criterion Assessment Grid

Criterion name: Network classes

Criticality principle: Impacts

Utilization principle: Give priority to links connecting particular network classes.

Comments:

- This criterion is intended as a follow-up to network class ranking in terms of impacts.
- The life support network class that is the most important based on the goals of the study must be determined.
- Current data is not sufficient to do this class ranking. System class values still must be validated.
- Eventually, intermeshed LSN classes will be given priority.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Origin network
- Destination network
- Determine origin and destination LSN classes

LSN value class				
A	**B**	**C**	**D**	**E**
3	3	3	3	3

Equation:

$$Vclink : \frac{ValRo + ValRd}{2}$$

- Rounded off to the nearest unit

Abbreviations:

Cvlink	Criterion value for the link being studied
ValNo	Value of the origin life support network
ValNd	Value of the destination life support network

Criterion Assessment Grid

Criterion name: Criticality of the components involved

Criticality principle: Impacts

Utilization principle: Give priority to links that involve critical or secondary components.

Comments:

- A definition of criticality is given.
- The criticality of the components is then determined by network managers.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Criticality of LSNo components
- Criticality of LSNd components

Scale and law:

- The most critical components will give rise to the most impacts.
- Determine the criticality of the component involved in the LSNo and LSNd

Component criticality scale:	
Very slightly critical component	**1**
Slightly critical component	**2**
Critical component	**3**
Very critical component	**4**
Extremely critical component	**5**

Equation:

$$Vclink = \frac{VcompO + VcompD}{2}$$

- Rounded off to the nearest unit

Abbreviation:

Cvlink	Criterion value for the link being studied
VcompO	Criticality value for component O
VcompD	Criticality value for component D

Criterion Assessment Grid

Criterion name: System efficiency

Criticality principle: Impacts

Utilization principle: Give priority to links with the most impacts on network operation – that is, links with the greatest change in network efficiency.

Comments:

- Efficiency reduction values are expressed in percentages.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Link direction
- Reduction in LSNo efficiency (RE) / Reduction in LSNd efficiency (RE)

Scale and law:

- The greater the reduction in network efficiency, the greater the increase in potential impacts on the network.

1. Determine the direction of the link.
2. Calculate the reduction in origin and/or destination efficiency.
3. Reduce the result to a scale of 5.
4. Round off the result to the nearest unit.

Equation if the link is Unidirectional:

$$Vclink = \left(\frac{DERSVd(\%)}{100} \right) * 5$$

Equation if the link is Bidirectional:

$$Vclink = \left(\frac{DERSVo(\%) + DERSVd(\%)}{200} \right) * 5$$

Abbreviations:

Cvlink	Criterion value for the link being studied
RLSNEo	Reduction in origin LSN efficiency
RLSNEd	Reduction in destination LSN efficiency

Criterion Assessment Grid

Criterion name: Potential domino effects

Criticality principle: Impacts

Utilization principle: Give priority to links whose failure or creation gives rise to domino effects.

Comments:

- Studies of impacts determine the number of networks connected to a link.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Link direction
- Number of networks connected to the *o* component (NNCo – including the link being studied)
- Number of networks connected to the *d* component (NNCd – including the link being studied)

Scale and law:

- The more domino effects the link generates, the more vulnerable it is considered to be.
- Determine the direction of the link.

Equation if the link is Unidirectional:
$SED = NRCo$

Equation if the link is Bidirectional:
$SED = (NRCo + NRCd)$

SDE	Cvlink
0	0
1	2
2	3
3	4
>3	5

Abbreviations:

Cvlink	Criterion value for the link being studied
NNCo	Number of networks connected to the origin component
NNCd	Number of networks connected to the destination component
SDE	Sum of domino effects

Criterion Assessment Grid

Criterion name: Alternative

Criticality principle: Impacts

Utilization principle: Give priority to links that have no alternative.

Application principle:

- This criterion does not apply to indirect links since they cannot have alternatives.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Existence of an alternative to this link

Scale and law:

- The fewer alternatives a link has, the greater the potential impacts.
- Determine whether the link has an alternative.

Alternative			
Alternative	Yes	No	Unav.
Cvlink	1	5	3
Indirect link	Inapplicable = 0		

Abbreviation:

Cvlink Criterion value for the link being studied
Unav. Unavailable

Criterion Assessment Grid

Criterion name: Authority

Criticality principle: Emergency management and measures

Utilization principle: Give priority to links without set responsibility.

Comments:

- Responsibility types must be adapted based on the geographic location of the LSNs.
- Cyberlinks are prioritized first since responsibility for these networks is often different from responsibilities for LSNs. Emergency measures management thus involves several players.
- Indirect links are then prioritized since loss of control over the material involves a further difficulty.
- Direct links are processed last since they are the best identified and controlled.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Nature of the link

Authority			
	Nature		
	I	C	D
Cvlink	5	5	1

Abbreviation:

Cvlink	Criterion value for the link being studied
I	Indirect links
D	Direct links
C	Cyberlinks

Criterion Assessment Grid

Criterion name: Preparation

Criticality principle: Emergency management and measures

Utilization principle: Give priority to links that have neither emergency measures nor exercises.

Comments:

- When exercises involving the link are carried out, it is understood that they involve both the origin and destination networks.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Importance attached to the link in case of emergency measures in the LSNo (IEMO)
- Importance attached to the link in case of emergency measures in the LSNd (IEMD)
- Importance attached to the link regarding preparatory exercises (IPE)

Scale and law:

- Piece of information not available = no
- LSNo
  1. The link is included in the emergency measures (yes/no)
  2. The link has been involved in exercises (yes/no)
- LSNd
  - Repeat steps 1 and 2.

Preparation			
EM		IPE	Cvlink
IEMO	IEMD		
No	No	Yes	4
		No	5
Yes	No	Yes	3
		No	4
No	Yes	Yes	3
		No	4
Yes	Yes	Yes	1
		No	2

Abbreviations:

Cvlink	Criterion value for the link being studied
LSNo	Origin life support network
LSNd	Destination life support network
EM	Emergency measures
IPE	Importance attached to preparatory exercises
IEMO	Importance attached to emergency measures in the LSNos
IEMD	Importance attached to emergency measures in the LSNds

Criterion Assessment Grid

Criterion name: Risk communication

Criticality principle: Emergency management and measures

Utilization principle: Give priority to links that have no communication measures.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Existence of a risk communication structure related to the risk.

Scale and law:

- Links without a communication network established by the networks are more vulnerable since information cannot be communicated when needed.

	Risk communication		
Communication structure	Yes	No	Unav.
Cvlink	0	5	4

Abbreviations:

Cvlink Criterion value for the link being studied
Unav. Unavailable

Criterion Assessment Grid

Criterion name: Link reaction time

Criticality principle: Emergency management and measures

Utilization principle: Give priority to links whose creation time allows for a reaction time.

Application principle: This criterion applies only to indirect links.

Comments:

- Link creation time, or the time needed to develop the link is determined by simulation or expertise.
- This creation time is associated with a reaction time that allows managers to react effectively to the creation of this link.
- The scale is determined based on variable times.
- Links where the creation time is shorter than management time are more vulnerable but they cannot be given priority because reaction might be less complete.

Parameters used:

- Link reaction time

Reaction time				
Time	**Short** (seconds)	**Medium** (minutes)	**Long** (hours)	**Inapplicable**
Cvlink	2	4	5	0

Abbreviations:

Cvlink Criterion value for the link being studied

Criterion Assessment Grid

Criterion name: Operational management

Criticality principle: Emergency management and measures

Utilization principle: Give priority to links with an operational management time.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Operational management time

Scale and law:

- The links with the longest operational management time should be given priority.

	Operational management time		
Time	**Yes**	**No**	**Unav.**
Cvlink	5	1	3

Abbreviations:

Cvlink Criterion value for the link being studied
Unav. Unavailable

Criterion Assessment Grid

Criterion name: Recovery time

Criticality principle: Management and emergency measure

Utilization principle: Give priority to links with a long recovery time since they are the hardest to manage.

Comments:

- For direct links and cyberlinks, recovery time is the time needed to repair the link.
- Recovery time for indirect links is defined as the time required for an LSNo to control the material carried by the link. That is when return-to-normal activities can begin.
- A scale is created based on variable times.

Weight of the criterion in ranking calculations: 1

Parameters used:

- Recovery time

Scale and law:

- Links with the longest recovery times cause greater difficulty as to emergency measures and should therefore be given priority.

	Recovery time		
Time	**Short** (minutes)	**Medium** (hours)	**Long** (days)
Cvlink	2	4	5

Abbreviations:

Cvlink Criterion value for the link being studied

Appendix B – Link Parameterization

Link description		
Link name		
Description		
Context		
Parameter	**Possible value**	**Value chosen**
Nature	Indirect / Direct / Cyberlink	
Extent of link	Length in km	
Direction	Unidirectional / Bidirectional	
Nature of LSNo components	Operational / Infrastructure	
Nature of LSNd components	Operational / Infrastructure	
Normal protection	Yes / No / Unavailable	
Exceptional protection	Yes / No / Unavailable	
LSNo network class	A/B/C/D/E	
LSNd network class	A/B/C/D/E	
LSNo component criticality	Extremely critical / Very critical / Critical / Slightly critical / Very slightly critical	
LSNd component criticality	Extremely critical / Very critical / Critical / Slightly critical / Very slightly critical	
Reduction in LSNo efficiency	%	
Reduction in LSNd efficiency	%	
Number of networks connected to the origin (NRCO)	Number greater than or equal to 0	
Number of networks connected to the destination (NRCD)	Number greater than or equal to 0	
Existence of an alternative	Yes / No / Unavailable	
Importance of emergency measures at origin (IEMO)	Yes / No / Unavailable	
Importance of emergency measures at destination (IEMD)	Yes / No / Unavailable	
Importance in preparatory exercises (IPE)	Yes / No / Unavailable	
Communications structure	Yes / No / Unavailable	
Reaction time	Time in minutes / hours / days / Inapplicable	
Operational management time (OMT)	Yes / No / Unavailable	
Recovery time	Time in minutes / hours / days	

Link description	
Link name	Link 1
Description	Telephone link used to transfer information between a municipality's fire and police departments
Context	It is hard to monitor this link since it is handled by two independent authorities. Its maintenance is essential to public security since it is used to coordinate various emergency and public safety teams.

Parameter	Possible value	Value chosen
Nature	Indirect / Direct / Cyberlink	Cyberlink
Extent of link	Length in km	0.5
Direction	Unidirectional / Bidirectional	Bidirectional
Nature of LSNo components	Operational / Infrastructure	O
Nature of LSNd components	Operational / Infrastructure	O
Normal protection	Yes / No / Unavailable	No
Exceptional protection	Yes / No / Unavailable	Yes
LSNo network class	A/B/C/D/E	E
LSNd network class	A/B/C/D/E	E
LSNo component criticality	Extremely critical Very critical Critical Slightly critical Very slightly critical	Extremely critical
LSNd component criticality	Extremely critical Very critical Critical Slightly critical Very slightly critical	Extremely critical
Reduction in LSNo efficiency	%	90
Reduction in LSNd efficiency	%	70
Number of networks connected to the origin (NRCO)	Number greater than or equal to 0	2
Number of networks connected to the destination (NRCD)	Number greater than or equal to 0	2
Existence of an alternative	Yes/No/Unavailable/Inapplicable	No
Importance of emergency measures at origin (IEMO)	Yes / No / Unavailable	Unav.
Importance of emergency measures at destination (IEMD)	Yes / No / Unavailable	Unav.
Importance in preparatory exercises (IPE)	Yes / No / Unavailable	Unav.
Communications structure	Yes / No / Unavailable	No
Reaction time	Time in minutes / hours / days / Inapplicable	Inapplicable
Operational management time (OMT)	Yes / No / Unavailable	No
Recovery time	Time in minutes / hours / days	2 hours

Link description			
Link name	Link 2		
Description	Link between an electricity distribution cable and a water purification station		
Context	This electric power link services a purification plant that serves an entire city. The plant, where the equipment is ageing, faces particular problems due to the large number of customers to be served. Generators are available, but there are not enough of them to solve the problems, even in the medium term.		
Parameter		**Possible value**	**Value chosen**
Nature		Indirect / Direct / Cyberlink	Direct
Extent of link		Length in km	3
Direction		Unidirectional / Bidirectional	Unidirectional
Nature of LSNo components		Operational / Infrastructure	I
Nature of LSNd components		Operational / Infrastructure	I
Normal protection		Yes / No / Unavailable	No
Exceptional protection		Yes / No / Unavailable	Yes
LSNo network class		A/B/C/D/E	A
LSNd network class		A/B/C/D/E	C
LSNo component criticality		Extremely critical Very critical Critical Slightly critical Very slightly critical	Slightly critical
LSNd component criticality		Extremely critical Very critical Critical Slightly critical Very slightly critical	Extremely critical
Reduction in LSNo efficiency		%	20
Reduction in LSNd efficiency		%	80
Number of networks connected to the origin (NRCO)		Number greater than or equal to 0	1
Number of networks connected to the destination (NRCD)		Number greater than or equal to 0	1
Existence of an alternative		Yes/No/Unavailable/Inapplicable	No
Importance of emergency measures at origin (IEMO)		Yes / No / Unavailable	No
Importance of emergency measures at destination (IEMD)		Yes / No / Unavailable	Yes
Importance in preparatory exercises (IPE)		Yes / No / Unavailable	No
Communications structure		Yes / No / Unavailable	Unav.
Reaction time		Time in minutes / hours / days / Inapplicable	Inapplicable
Operational management time (OMT)		Yes / No / Unavailable	Yes
Recovery time		Time in minutes / hours / days	2 days

Link description		
Link name	Link 3	
Description	Cyberlink between a computer network and electricity production facilities	
Context	This cyberlink allows volume and electricity production reservoir quality control to be automated by regularly measuring water levels. Its failure could lead to floods or deprive the community of water. Moreover, malicious acts might play an important role since cyberlinks are more vulnerable to this potential problem.	
Parameter	**Possible value**	**Value chosen**
Nature	Indirect / Direct / Cyberlink	Cyberlink
Extent of link	Length in km	2
Direction	Unidirectional / Bidirectional	Unidirectional
Nature of LSNo components	Operational / Infrastructure	O
Nature of LSNd components	Operational / Infrastructure	O
Normal protection	Yes / No / Unavailable	No
Exceptional protection	Yes / No / Unavailable	Yes
LSNo network class	A/B/C/D/E	A
LSNd network class	A/B/C/D/E	C
LSNo component criticality	Extremely critical Very critical Critical Slightly critical Very slightly critical	Very slightly critical
LSNd component criticality	Extremely critical Very critical Critical Slightly critical Very slightly critical	Extremely critical
Reduction in LSNo efficiency	%	10
Reduction in LSNd efficiency	%	50
Number of networks connected to the origin (NRCO)	Number greater than or equal to 0	0
Number of networks connected to the destination (NRCD)	Number greater than or equal to 0	1
Existence of an alternative	Yes/No/Unavailable/Inapplicable	Yes
Importance of emergency measures at origin (IEMO)	Yes / No / Unavailable	No
Importance of emergency measures at destination (IEMD)	Yes / No / Unavailable	No
Importance in preparatory exercises (IPE)	Yes / No / Unavailable	No
Communications structure	Yes / No / Unavailable	Yes
Reaction time	Time in minutes / hours / days / Inapplicable	Inapplicable
Operational management time (OMT)	Yes / No / Unavailable	Yes
Recovery time	Time in minutes / hours / days	Minutes

Link description	
Link name	Link 4
Description	Link between gas pipelines and water pipes
Context	This indirect link is hard to evaluate. In many places, water and gas pipes cross and co-exist. Sometimes, leaks from one network can influence the other through a domino effect. For this link, it is important that gas not reach the water pipes since that would deprive a significant proportion of the population of water.

Parameter	Possible value	Value chosen
Nature	Indirect / Direct / Cyberlink	Indirect
Extent of link	Length in km	0.005
Direction	Unidirectional / Bidirectional	Unidirectional
Nature of LSNo components	Operational / Infrastructure	I
Nature of LSNd components	Operational / Infrastructure	I
Normal protection	Yes / No / Unavailable /	Unav.
Exceptional protection	Yes / No / Unavailable	No
LSNo network class	A/B/C/D/E	B
LSNd network class	A/B/C/D/E	C
LSNo component criticality	Extremely critical Very critical Critical Slightly critical Very slightly critical	Very critical
LSNd component criticality	Extremely critical Very critical Critical Slightly critical Very slightly critical	Very critical
Reduction in LSNo efficiency	%	60
Reduction in LSNd efficiency	%	5
Number of networks connected to the origin (NRCO)	Number greater than or equal to 0	1
Number of networks connected to the destination (NRCD)	Number greater than or equal to 0	1
Existence of an alternative	Yes/No/Unavailable/Inapplicable	Inapplicable
Importance of emergency measures at origin (IEMO)	Yes / No / Unavailable	Unav.
Importance of emergency measures at destination (IEMD)	Yes / No / Unavailable	Yes
Importance in preparatory exercises (IPE)	Yes / No / Unavailable	No
Communications structure	Yes / No / Unavailable	No
Reaction time	Time in minutes / hours / days / Inapplicable	4 minutes
Operational management time (OMT)	Yes / No / Unavailable	Yes
Recovery time	Time in minutes / hours / days	3 days

Link Description	
Link name	Link 5
Description	Link connecting an electric power distribution network to a subway network
Context	This link provides people with safe transportation. Its failure would prevent workers from participating normally in socio-economic activities.

Parameter	Possible value	Value chosen
Nature	Indirect / Direct / Cyberlink	Direct
Extent of link	Length in km	15 km
Direction	Unidirectional / Bidirectional	Unidirectional
Nature of LSNo components	Operational / Infrastructure	I
Nature of LSNd components	Operational / Infrastructure	I
Normal protection	Yes / No / Unavailable	Yes
Exceptional protection	Yes / No / Unavailable	Yes
LSNo network class	A/B/C/D/E	A
LSNd network class	A/B/C/D/E	A
LSNo component criticality	Extremely critical Very critical Critical Slightly critical Very slightly critical	Slightly critical
LSNd component criticality	Extremely critical Very critical Critical Slightly critical Very slightly critical	Extremely critical
Reduction in LSNo efficiency	%	5
Reduction in LSNd efficiency	%	95
Number of networks connected to the origin (NRCO)	Number greater than or equal to 0	0
Number of networks connected to the destination (NRCD)	Number greater than or equal to 0	0
Existence of an alternative	Yes/No/Unavailable/Inapplicable	No
Importance of emergency measures at origin (IEMO)	Yes / No / Unavailable	No
Importance of emergency measures at destination (IEMD)	Yes / No / Unavailable	Yes
Importance in preparatory exercises (IPE)	Yes / No / Unavailable	Yes
Communications structure	Yes / No / Unavailable	Yes
Reaction time	Time in minutes / hours / days / Inapplicable	Inapplicable
Operational management time (OMT)	Yes / No / Unavailable	No
Recovery time	Time in minutes / hours / days	2 hours

Appendix C – Validation

The methodology to be used to determine the value of each criterion (Cvlink) and the total value of the link (Tvlink) is explained below. Link 1 will be used as an example to illustrate the steps of the methodology:

1. Calculation of the value of each criterion;
2. Calculation of the total link value;
3. Calculation of maximum link value; and
4. Identification of criticality level interval limits.

1. Calculation of the value of each criterion

Criterion 1
Name: Nature
Parameter: Nature = Link 1 is a cyberlink.
Criterion value: Since Link 1 is a cyberlink, Cvlink 1 = 3.

Criterion 2
Name: Geographic corridor
Parameter: Geographic area = Link 1 is 0.5 km long.
Criterion value: Since Link 1 is < 2 km, Cvlink 2 = 1.

Criterion 3
Name: Direction
Parameters: Direction = Link 1 is bidirectional.
Nature = Link 1 is a cyberlink.
Criterion value: Since Link 1 is a cyberlink and is bidirectional, Cvlink 3 = 4.

Criterion 4
Name: Impregnation
Parameters: The nature of the components involved at the origin is operational.
The nature of the components involved at the destination is operational.
Criterion value: Since Link 1 involves operational components at the origin and destination, Cvlink 4 = 5.

Criterion 5
Name: Protection in normal situations
Parameters: Nature = Link 1 is a cyberlink.
Existence of normal protection = the link has no protection measures.
Criterion value: Since Link 1 is a cyberlink and has no protection measures in normal situations, Cvlink 5 = 5.

Criterion 6
Name: Mitigation
Parameters: Nature = Link 1 is a cyberlink.
Existence of exceptional protection = Yes
Criterion value: Since Link 1 is a cyberlink and has exceptional means of protection, Cvlink 6 = 1.

Criterion 7
Name: Associated vulnerabilities
Parameters: Nature = Link 1 is a cyberlink
Nature of components affected at the LSNo = operational.
Nature of components affected at the LSNd = operational.
Link 1 direction is bidirectional.
Criterion value: Since Link 5 is a bidirectional cyberlink and the components affected at LSNo and LSNd are operational, Cvlink 7 = 5.

Criterion 8
Name: Network class
Parameter: LSNo class = public security
LSNd class = public security
Criterion value: Since Link 1 involves two class 5 LSNs, Cvlink 8 = 3.

Criterion 9
Name: Criticality of the components involved
Parameters: Criticality of components involved at the LSNo = extremely critical.
Criticality of components involved at the LSNd = extremely critical.
Criterion value: Since Link 1 affects two very critical components, Cvlink 9 = 5.

Criterion 10
Name: Network efficiency
Parameters: Link direction = bidirectional
Reduction in efficiency (RE) at the origin LSN = 90 %
Reduction in efficiency (RE) at the destination LSN = 70 %
Criterion value: Since Link 1 is bidirectional and the efficiency difference of LSNo is 90% and the efficiency difference of LSNd is 70 %, Cvlink 10 = [((90+70)/200)*5] = 4.

Criterion 11
Name: Potential domino effects
Parameters: Link direction = bidirectional
Number of networks connected at the origin (NNCo) = 2
Number of networks connected at the destination (NNCd) = 2
Criterion value: Since Link 1 is bidirectional and NNCo + NNCd = 4, Cvlink 11 = 5.

Criterion 12
Name: Alternative
Parameter: Existence of an alternative = no
Criterion value: Since Link 1 has no alternative,Cvlink 12 = 5.

Criterion 13
Name: Authority
Parameter: Nature = Link 1 is a cyberlink.
Criterion value: Since Link 1 is a cyberlink, Cvlink 13 = 5.

Criterion 14
Name: Preparation
Parameter: Importance attached to emergency measures at LSNo (IEMo) = no
Importance attached to emergency measures at LSNd (IEMd) = no
Importance attached to preparatory exercises (IPE) = no
Criterion value: Since we cannot determine whether Link 5 is protected in IEMO, IEMD or IPE, Cvlink 14 = 5.

Criterion 15
Name: Risk communication
Parameter: Existence of communication for Link 1 = no.
Criterion value: Since Link 5 has no communications structure, Cvlink 15 = 5.

Criterion 16
Name: Reaction time
Parameter: Reaction time = not applicable since Link 1 is a cyberlink.
Criterion value: Since this criterion does not apply to cyberlinks, Cvlink 16 = 0.

Criterion 17
Name: Operational management
Parameter: Operational management time for Link 1= null.
Criterion value: Since Link 1 has no operational management time, Cvlink 17 = 1.

Criterion 18
Name: Recovery time
Parameter: Recovery time = 2 hr.
Criterion value: Since the average time needed to re-establish Link 1 is 2 hours, Cvlink 18 = 4.

2. Calculation of the total link value

When the value of each criterion for the link being studied has been determined, these values must be added to obtain the total value of the link.

$$VTlink = \sum_{j=1}^{n}\left[Pclj * \left(\sum_{i=1}^{m} (Pji * Vlinkij) \right) \right]$$

VT*link* = 3+1+4+5+5+1+5+3+5+4+5+5+5+5+5+0+1+4

VTlink = 66

The total value for Link 1 is therefore 66.

3. Calculation of the maximum link value

The maximum value (MaxVal) is found by multiplying the number of criteria used by the maximum value that can be assigned to each criterion – this is, 5.

$$ValMax = \sum_{j=1}^{n} Pclj * \left(\sum_{i=1}^{m} (Pji * 5) \right)$$

Thus, for Link 1, the maximum value = 18 * 5 = 90

4. Identification of criticality level interval limits

There are five levels of criticality. To determine the size of these intervals, we need only divide the maximum value by 5.

Bi = MaxVal / 5

Thus, for Link 1, the intervals are Bi = 90 / 5= 18

The maximum value must then be divided into the following five intervals:

- Interval 1: Very slightly critical = [0;*Bi*]
- Interval 2: Slightly critical =]*Bi*; *2Bi*]
- Interval 3: Critical =]2*Bi*; 3*Bi*]
- Interval 4: Very critical =]3*Bi;* 4*Bi]*
- Interval 5: Extremely critical =]4*Bi*; 5*Bi*]

For Link 1, the criticality level intervals are:

- Interval 1: Very slightly critical = [0, 18]
- Interval 2: Slightly critical =]18, 36]
- Interval 3: Critical =]36, 54]
- Interval 4: Very critical =]55, 72]
- Interval 5: Extremely critical =]72, 90]

Link 1 is thus in Interval 4 since it has a total value of 66. It is then possible to state that in an overall evaluation, it is very critical to give priority to processing this link when planning and implementing emergency measures.